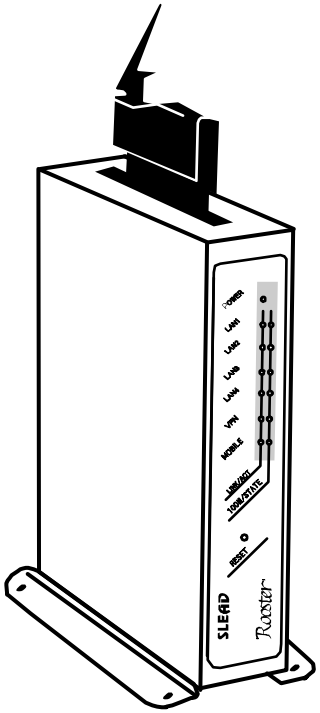
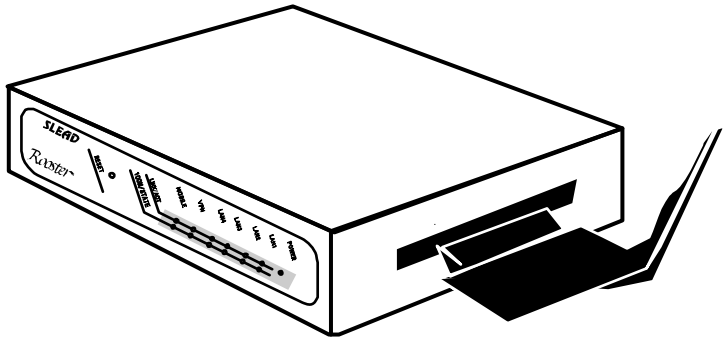
モバイルデータ通信カード対応　高信頼性 VPN モバイルルータ

Rooster - VMII

SC-RS920VM2

取扱説明書





http://www.sun-denshi.co.jp/sc/

Rooster-VMII

取扱説明書 目次

- はじめに 1
- 安全上のご注意（必ずお守りください。） 1

1. Rooster-VMⅡ概要 4
1.1 主な特長 4
1.2 Rooster-VMⅡ 設定フロー 5
1.3 同梱品の確認 5
1.4 各部の名称と機能 6
1.5 ランプの状態と働き 7

2. Rooster-VMⅡの導入 7
2.1 Rooster-VMⅡの接続方法 7
2.1.1 必要な環境 7
2.1.2 接続方法 7
2.2 ご利用環境の確認 8
2.3 パソコンの設定（TCP/IP の設定等） 8
2.3.1 DHCP を使用する設定（Windows XP の場合） 8

3. Rooster-VMⅡの初期設定 9
3.1 Rooster 設定ツールへのログイン方法 9
3.2 LAN 側の設定 10
3.3 ログインパスワードの設定 11
3.4 時刻の設定 11
3.4.1 NTP サーバを使用して定期的に時刻を同期する場合 12
3.4.2 手動で時刻の設定を行う場合 12
3.5 メールアカウントの設定 12
3.6 電源制御 13

4. ダイヤルアップ設定 14
4.1 プロバイダ情報の確認 14
4.2 ダイヤルアップ接続設定 14
4.2.1 ダイヤルアップ接続先の追加、変更方法 16
4.3 接続/切断方法 17
4.3.1 通信ステータス詳細表示 18
4.4 対応通信モード一覧 19
4.4.1 インターネット接続の料金コースと専用通信方式 19
4.4.2 PIAFS 通信方式 20

5. 着信設定 20
5.1 RAS 着信接続設定 20
5.1.1 着信番号での認証設定 23
5.1.2 RAS 着信時のステータス表示 23
5.2 ダイヤルアップ接続設定と RAS 着信設定の併用 24
5.3 WakeOn 着信設定 25
5.3.1 着信番号での認証設定 26

6. Rooster-VMⅡ メンテナンス 27
6.1 設定情報の保存、読み込み 27
6.1.1 現在の設定を保存 27
6.1.2 保存した設定の読み込み 27
6.2 設定情報の消去 27
6.3 ファームウェアのアップデート方法 27
6.4 Rooster-VMⅡの再起動 28
6.5 メンテナンスポート 28

7. 各種サービス設定 29
7.1 アドレス解決機能 29
7.1.1 IP アドレスを指定メールアカウントに通知する設定 29
7.1.2 ダイナミック DNS サーバを利用する設定 30
7.2 DNS サービス 31
7.3 DHCP サービス 31
7.4 TELNET サービス 32
7.5 Web サービス 33
7.6 QoS 33
7.6.1 QoS 機能の追加設定 34
7.7 SNMP 35
7.8 WAN ハートビート機能 36
7.9 ログ管理 36

8. ネットワーク設定 37
8.1 VPN パススルー 37
8.2 スタティックルーティング 37
8.3 フィルタリング 38
8.4 バーチャルサーバ 40
8.5 DMZ 41

9. VPN 設定 41
9.1 VPN 設定 41
9.2 VPN 通信の接続/切断方法 43
9.2.1 2 点間の WAN 側 IP アドレスが固定の場合 44
9.2.2 WAN 側 IP アドレスの一方が固定、Rooster-VMⅡが動的の場合 45

10. ログの参照方法 45
10.1 パケット通信ログ 45
10.1.1 パケット通過ログ 45
10.1.2 パケット遮断ログ 46
10.2 回線ログ 46
10.2.1 モバイルカードログ 46
10.2.2 VPN ログ 47
10.3 サービスログ 48
10.3.1 アドレス解決ログ 48
10.3.2 DHCP ログ 48
10.3.3 WAN ハートビートログ 49
10.3.4 PPP ログ 49
10.4 その他ログ 50
10.4.1 システムログ 50

- **製品仕様 51**
- **サポートのご案内 53**

はじめに

表記について

本取扱説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しております。

⚠警告	人体に危険を及ぼしたり、装置に大きなダメージを与えたりする可能性があることを示しています。必ずお守りください。
ⓘ注意	機能停止を招いたり、各種データを消してしまったりする可能性があることを示しています。十分に注意してください。
☼メモ	関連情報です。参考にお読みください。

商標について

「Rooster」「Sun Communications」は、サン電子株式会社の登録商標および商標登録出願中です。
その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。
本文中の各社の商標または登録商標には、TM、®マークは表示しておりません。

GPL/LGPL ライセンスについて

本製品は、GPL/LGPLの適用ソフトウェアを使用しております。オープンソースとしての性格上著作権による保証はなされておりませんが、本製品につきましては保証書、および取扱説明書記載の条件により当社による保証がなされています。
GPL/LGPLのライセンスにつきましては、以下のURLをご覧ください。

- http://www.gnu.org/licenses/gpl.html
- http://www.gnu.org/licenses/lgpl.html

変更済みGPL対象モジュール、その配布方法につきましては、サン電子㈱サンコミュニケーションズ事業部 サポートセンターにご連絡ください。なお、配布時発生する費用はお客様のご負担となります。

☞本取扱説明書の画面イメージは開発中のものです。
実際の画面とは多少異なる場合があります。

安全上のご注意（必ずお守りください。）

■ **ここに記載している注意事項は、安全に関わる重要な内容ですので、必ず守ってください。本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。**

⚠警告	この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠注意	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関する拡大損害を示しています。
⃠	禁止行為（してはいけないこと）を示しています。
❗	強制行為（必ずしなければいけないこと）を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

⚠警告

分解禁止

本製品を分解したり、改造したりしないでください。

⇒感電、火災、故障の原因になります。

禁止

近くに雷が発生したときには AC アダプタをコンセントから抜いてご使用をお控えください。

⇒落雷が火災、感電、故障の原因となるときがあります。

禁止

本製品に水などの液体をかけたり、異物を入れたりしないでください。⇒感電や火災の原因になります。

万一、本製品に液体がかかったり、異物が入ったりした場合は、AC アダプタをコンセントから抜いて、点検修理を依頼してください。

強制

製品から煙、異臭、異常音が発生した場合は、AC アダプタをコンセントから抜き、本製品を接続している機器からケーブルを取り外してください。また、修理、点検を依頼してください。

⇒火災の原因になります。

禁止

電源ケーブルを傷つけないでください。

⇒感電、火災の原因になります。

強制

AC アダプタは、AC100V コンセントに接続してください。また、本製品を設置、移動する時は、電源プラグを抜いてください。

⇒故障、火災の原因になります。

禁止

梱包のポリ袋などは、小さいお子様の手の届く所に置かないでください。

⇒小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。

強制

電源プラグは確実に根元まで差し込んでください。また、電源プラグとコンセントの間のほこりは、定期的（半年に一回程度）に取り除いてください。

⇒電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。

⚠注意

禁止

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

⇒本製品の故障や破損などによって、発煙、発火、感電の原因になります。下記の環境には、特にご注意ください。

- 室内または製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所

禁止

同梱の AC アダプタ以外の電源を使用しないでください。

⇒他の電源を使用すると、故障、火災の原因になります。

強制

30cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

⇒そのまま使用すると、重大な事故になる可能性があります。

ご使用にあたってのお願い

- **本製品周辺で静電気的障害を発生させないでください。**

  ⇒本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。

- **本製品はていねいに取り扱ってください。**

  ⇒本製品に強いショックを与えると破損の原因になります。

- **本製品のお手入れは、電源を切った状態で行ってください。**

  ⇒誤動作や故障の原因になります。

- **本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。**
  汚れがひどい場合は、柔らかい布に台所中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。

  ⇒揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。

地球環境保全のため、次のことにご協力ください。

- 本製品および付属品は、不燃物として処分してください。
- 廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
- 一般ごみとして、家庭で焼却処分しないでください。
  ダイオキシンや塩化水素ガスなどが発生し、環境や人体に影響を与えます。

ご注意

- **本製品の仕様は国内向けになっておりますので、海外ではご利用になれません。**

  These products are designed for use in Japan only and cannot be used in any other countries.

- **本製品は、パソコンなどの OA 機器に使用することを目的に設計、製造されています。**
  医療機器や幹線通信機器、電算機システムなどの、きわめて高い安全性や信頼性が要求される用途には使用しないでください。

- **取扱説明書について、次の点にご注意ください。**

1. 本製品は各通信事業者のモバイルカードを利用して無線によるデータ通信を行う事が出来る装置です。本製品及びモバイルカード等の不具合、誤動作又は停電、回線障害、その他の外部要因によって通信障害が発生した為に生じた損害等については、当社としては責任を負いかねますので、予めご了承ください。
2. 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
3. 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
4. 本取扱説明書の内容につきましては、万全を期して作成致しましたが、万一ご不審な点や、ご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点等ございましたら、当社までご連絡ください。
5. 適用した結果の影響につきましては、3 項にかかわらず責任を負いかねますので、ご了承ください。
6. 本取扱説明書で指示されている内容につきましては、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害につきましては、保証期間内であっても責任を負いかねますので、ご了承ください。

1. Rooster-VMⅡ概要

1.1 主な特長

- **耐環境性能が大幅に向上**

  厳しい環境下での安定した運用を行う事が出来る耐環境性能の向上を図るため、ハードウェアの全面リニューアルを行いました。耐ノイズ、耐静電気性能などを大幅に向上させ、自動販売機、映像監視装置などへの組み込みによる無人環境において移動体通信による安定運用を実現する各種機能を新たに搭載しました。

- **長期間の安定運用を実現する各種電源制御機能**

  ハードウェアの耐環境性能向上に加え「Roosterの電源を35時間または6日毎にハードウェア処理で電源OFF/ONさせる」機能、「Roosterを1～6日毎にソフトウェア処理で自動電源OFF/ONさせる」機能を新たに搭載しました。
  これらの機能により、Roosterの電源を定期的にOFF/ONさせる事で、長期間の安定した運用が可能になり、無人拠点に設置される場合でも安心してご利用いただけます。

- **強力なウォッチドッグ機能**

  Rooster本体のCPUに何らかの影響を受けて正常な動作が不能になった場合には、即座に電源をOFF/ONするハードウェアウォッチドッグ機能を実装しました。

- **モバイルデータ通信カードのステータス情報取得機能（TELNET のみ）**

  モバイルデータ通信カード接続時、カードの電話番号、電界強度、位置情報（経度・緯度）をTELNETにて取得可能です。
  ※モバイルデータ通信カードの電源投入時の情報が取得できます。

- **Unnumbered 機能**

  Unnumbered機能に対応しておりますので、RoosterのWAN側にIPアドレスを付与することなく接続することが可能です。

- **Rooster-VMⅡ同士による対向通信を可能とする LAN 接続機能**

  Rooster-VMⅡ同士での対向通信を行うことが可能です。
  ダイヤルアップによる発信および、リモートアクセスによる着信の両モードで動作することが可能ですので、双方のRooster-VMⅡが発着信しあうことが可能になります。またMPPEプロトコルによるデータの暗号化も可能です。

- **認証プロトコル MS-CHAPv2 に対応**

  Rooster-VMⅡ同士での対向通信など、回線交換方式での接続時にMS-CHAPv2による認証が可能です

- **MPPE による暗号化機能**

  Rooster-VMⅡ同士での対向通信など、回線交換方式での接続時にMPPEプロトコルによる128bitでの暗号化が可能です。

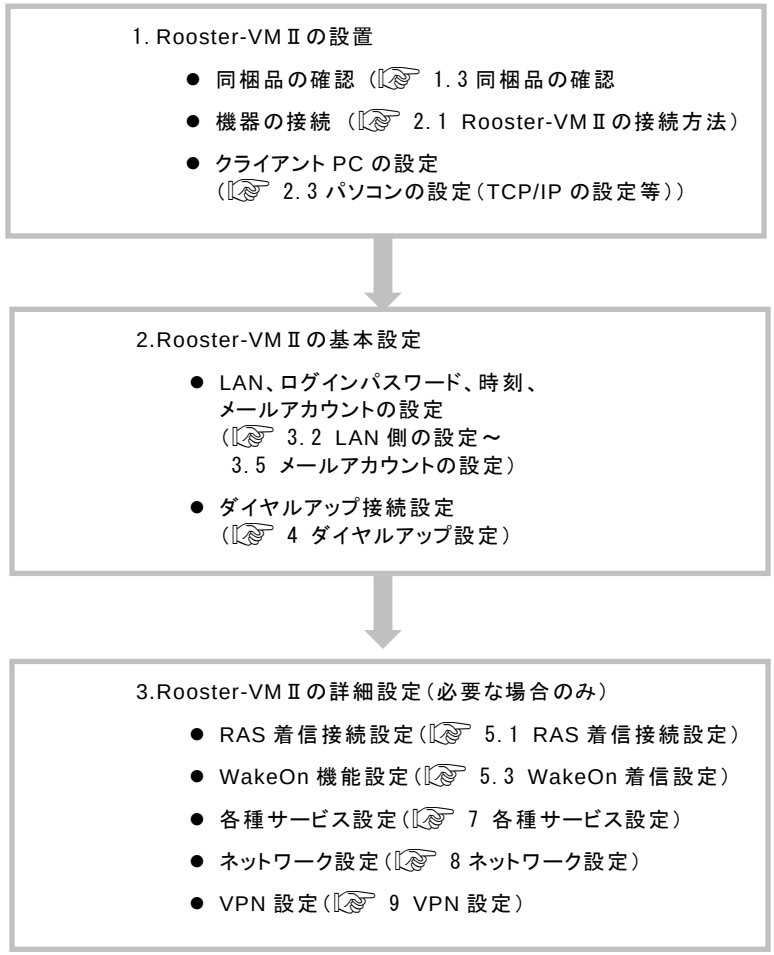
- **ハードウェア処理による VPN(IPsec)機能を標準搭載**

  Rooster-VMⅡでは、IPsecによるVPN機能を用いて、これまでモバイル環境では難しかったインターネットVPNの構築を可能としました。これにより、モバイルによる安全で高速な多拠点ネットワークを簡単に構築することができるようになります。
  Rooster-VMⅡでは、データの暗号化に3DES、認証方式にはSHA-1を採用しております。
  また、接続先相手の認証プロトコルにIKEを採用し、メインモード、アグレッシブモードのいずれにも対応しておりますので、さまざまなインターネットへの接続形態に対応することが可能です。
  IPsecによるVPN機能で、インターネットを利用した高セキュリティなテレメトリングへの応用も可能となります。

- **帯域制御および優先制御可能な QoS 機能を搭載**
- **安定した高度な運用を可能にする運用サポート機能を搭載**
  - WAN ハートビート機能
  - SNMP 機能
  - SYSLOG 機能
  - 各種ログ機能
  - RTC 機能
- **柔軟な設定管理機能**
- **セッションキープ／キープアライブ機能**
- **豊富なルーティング機能**
- **DHCP サーバ／クライアント／リレー機能**
- **WakeOn Voice 機能**
- **フィルタリング機能**
- **アドレス解決機能**
- **ダイナミック DNS 機能**

1.2 Rooster-VMⅡ 設定フロー

Rooster-VMⅡを使用してダイヤルアップ接続を行う場合、最低限2までの設定を行ってください。3の設定は、必要に応じて行ってください。



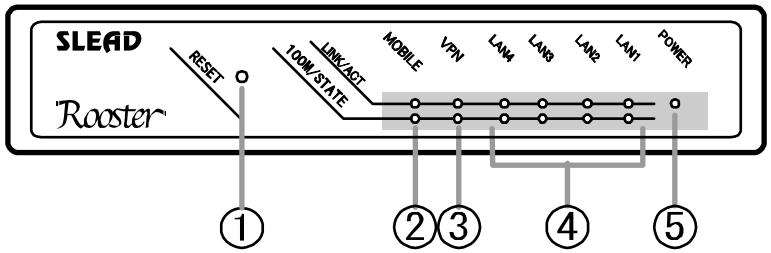
1.3 同梱品の確認

パッケージには、次のものが同梱されています。
万一不足しているものがありましたら、お買い求めの販売店、もしくはサポートセンターにご連絡ください。

● Rooster-VMⅡ本体	1 台
● スタートアップマニュアル	1 部
● CD-ROM (本取扱説明書、TELNET 設定機能説明書 収録)	1 枚
● 保証書	1 通
● AC アダプタ	1 個
● UTP ケーブル(カテゴリ 5 ストレート)	1 本
● 電源プラグ抜け防止クランプ	1 個
● 本体固定用ステー	2 枚
● モバイルカード保護板	1 枚
● FG 用ネジ	1 個
● 固定用ネジ (固定用ステー用×4、PC カード保護板用×2)	6 個
● ゴム足	4 個

1.4 各部の名称と機能

前面



背面

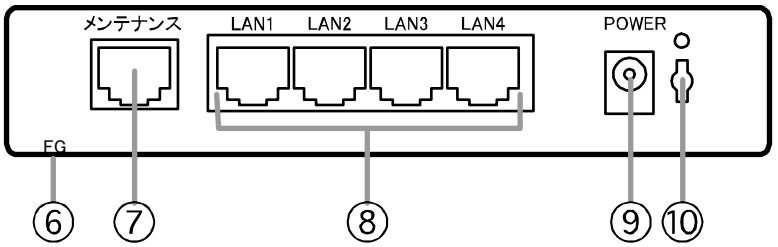


図 1-1　Rooster-VMⅡ 各部名称

- それぞれのランプの状態は、☞ 1.5ランプの状態と働きをご覧ください。

1. RESET スイッチ

   先の細いピンなどを使って6秒以上押し続けると、MOBILEランプ緑、橙共に点滅し、工場出荷時の設定に戻り、再起動します。

2. MOBILE ランプ

   モバイルカードの動作状態が表示されます。

3. VPN ステータスランプ

   VPNセッションの動作状態が表示されます。

4. LAN1～4 ランプ

   LAN1～4 ポート(⑧)へのLAN接続機器の接続状態が表示されます。

5. POWER ランプ

   Rooster-VMⅡの通電状態が表示されます。

6. FG 端子

   アース線を接続します。

7. メンテナンスポート

   設定専用のポートです。
   各種設定をメンテナンスポートからのみ行うようにすることもできます。

8. LAN1～4 ポート

   LAN(UTP)ケーブルで、LAN接続機器およびハブ等を接続します。

9. POWER コネクタ

   付属のACアダプタを接続します。

10. クランプ取り付け穴

    電源プラグ抜け防止クランプを取り付ける穴です。

☞電源プラグ抜け防止クランプの使い方

1. クランプを取り付けます。
2. AC アダプタを接続します。
3. クランプを閉じます。

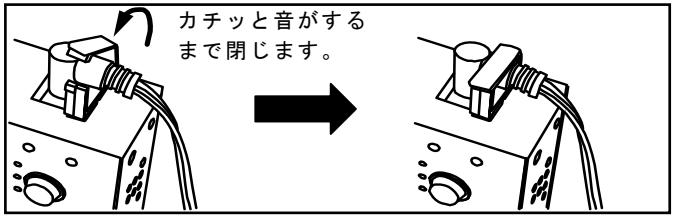


図 1-2　電源プラグ抜け防止クランプ取り付け方法

1.5 ランプの状態と働き

- MOBILE ランプ

ランプ	状態
緑点滅	ダイヤルアップ接続で、データ通信が行われている状態です。
緑点灯	ダイヤルアップ接続が確立された状態です。
緑消灯	ダイヤルアップ接続が行われていません。
橙点灯	ダイヤルアップ接続先での認証が確立された状態です。
橙点滅	電話を掛けている(オンフック)状態です。
橙消灯	電話を掛けていない(オフフック)状態です。

- VPN ステータスランプ

ランプ	状態
緑点滅	VPN 接続が確立され、データ通信が行われている状態です。
緑点灯	VPN 接続が確立された状態です。
緑消灯	VPN 接続が行われていません。

- LAN1～4 ランプ

ランプ	状態
緑点滅	LAN 接続機器とのデータ通信が行われている状態です。
緑点灯	LAN 接続機器が通電されていて、接続されている状態です。
緑消灯	LAN 接続機器が通電されていないか、ケーブルが外れています。
橙点灯	LAN 接続機器と 100Mbps で接続されている状態です。
橙消灯	LAN 接続機器 10Mbps で接続されている状態か、何も接続されていない状態です。

- POWER ランプ

ランプ	状態
緑点灯	電源が入っていて、使用可能な状態です。
緑消灯	電源が入っていません。

2. Rooster-VMⅡの導入

2.1 Rooster-VMⅡの接続方法

2.1.1 必要な環境

- TCP/IP が利用できる OS(Windows、MacOS、各種 UNIX など)を搭載し、Ethernet ポートを搭載したパソコン。
- LAN(UTP)ケーブル
- Internet Explorer 6.0 以上のブラウザ
  (上記以外のブラウザでは、正常に動作しない可能性があります。)

2.1.2 接続方法

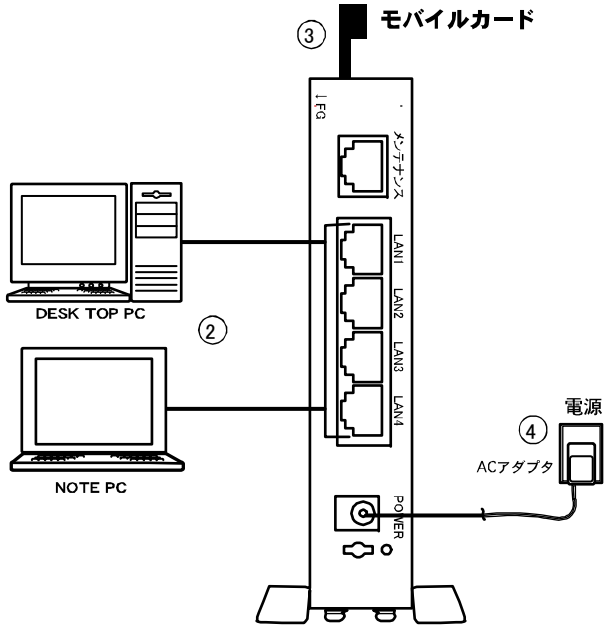


図 2-1 Rooster-VMⅡ 接続図

1. Rooster-VMⅡとパソコンの電源が入っていないことを確認してください。
2. LAN ポートにクライアントとなるパソコンを接続してください。
3. モバイルカードを接続してください。
4. Rooster-VMⅡの電源コネクタに AC アダプタを接続してください。
   次に AC アダプタをコンセントに接続してください。
5. パソコンの電源を入れてください。

注意

- Rooster-VMⅡは、モバイルカード専用ルータです。
  有線ブロードバンド回線に接続する機能は搭載しておりません。
- モバイルカードは、必ず電源を切った状態でカードの抜き差しを行ってください。電源を入れた状態でカードの抜き差しを行うと、Rooster-VMⅡが作動しません。
- AC アダプタは、必ず付属のものを使用してください。
  付属以外の AC アダプタを使用すると、故障・誤作動の原因になります。
  付属以外の AC アダプタを使用された場合の故障は、保証対象外となりますのでご了承願います。

2.2 ご利用環境の確認

Rooster-VMⅡとパソコンを接続するためにはパソコンにLAN環境が必要です。
LAN環境が無い場合には、ご利用のパソコンにあわせてLAN機器をご用意ください。

- パソコンで LAN ポートが標準で装備されていない場合、LAN アダプタをご利用のパソコンにあわせて増設してください。

インターネット接続の場合、通信事業者との契約が完了している必要があります。
以下についてご確認願います。

- モバイルカード等の回線事業者との契約、工事が完了している必要があります。
  （(株)NTT ドコモ、(株)ウィルコムなど）
- インターネット接続サービスであるプロバイダへの契約の完了している必要があります。
  （OCN、@nifty 等）
  事業者によっては回線事業者とプロバイダが同じ契約の場合があります。
  その場合別途プロバイダへの契約は必要ありません。
- Rooster-VMⅡの設定には、以下の情報が必要になります。プロバイダとの契約時に提供されている情報をご用意ください。
  不明な場合はご契約のプロバイダへお問い合わせください。
  - **アクセスポイントへの電話番号**
  - **ユーザー名**
  - **パスワード**
  - **ネームサーバ（DNS サーバ）の IP アドレス（設定が必要な場合）**

注意 アクセスポイントへの電話番号は、料金コースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。

2.3 パソコンの設定（TCP/IPの設定等）

Rooster-VMⅡにアクセスできるように、クライアントパソコンにDHCPクライアントの設定をします。
DHCPを使用しない場合は、各パソコンに手動でIPを設定する必要があります。その方法は、ネットワークカード及びWindowsのマニュアル等をご覧ください。

2.3.1 DHCPを使用する設定（Windows XPの場合）

1. コントロールパネルを開き、[ネットワークとダイヤルアップ接続]を選び、[ネットワーク接続]をダブルクリックして開きます。
   (クラシック表示の場合は、コントロールパネルを開いた後、[ネットワーク接続]のアイコンをクリックします。)

図 2-2 ネットワーク接続

2. 「ローカルエリア接続」を右クリックし、[プロパティ]をクリックします。
   ローカルエリア接続のプロパティが表示されます。

図 2-3 ローカルエリア接続のプロパティ

3. 「インターネットプロトコル（TCP/IP）」選び、[プロパティ]をクリックします。
   TCP/IPプロパティダイアログが表示されます。
4. 「IP アドレスを自動的に取得する」、「DNS サーバのアドレスを自動的に取得する」を選択します。

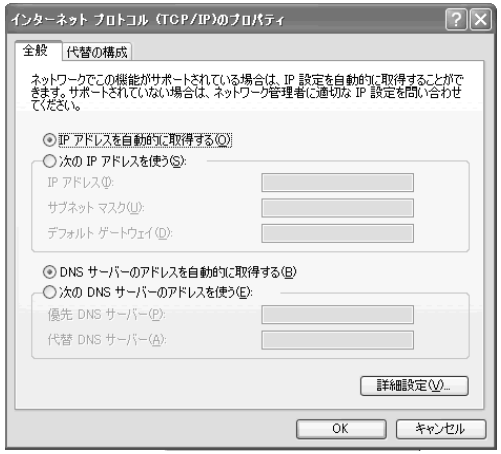


図 2-4　TCP/IP のプロパティ

5. [OK]をクリックしてダイアログを閉じます。
   [ローカルエリア接続のプロパティ]画面も、[OK]をクリックして閉じます。

3. Rooster-VMⅡの初期設定

3.1 Rooster設定ツールへのログイン方法

1. WWW ブラウザを起動します。
2. WWW ブラウザのアドレス入力欄に、Rooster-VMⅡの LAN 側 IP アドレス「**http://192.168.62.1/**」（工場出荷時状態）を入力し、Enter を押します。

図 3-1　Rooster-VMⅡ IP アドレスの入力

ログインダイアログボックスが表示されます。

図 3-2　ネットワークパスワードの入力画面

3. ユーザー名に「admin」、パスワードに「1234」(工場出荷時状態)と入力した後、OK ボタンをクリックします。
4. Rooster-VMⅡの設定ツールが表示されます。

注意

- 設定ツールは JavaScript を使用しています。
  ブラウザの JavaScript をオンにしてから設定を行ってください。
- 設定ツールを表示し、しばらく放置すると、一旦ログアウト処理を行います。その後、設定ツールにアクセスすると、再度ログインダイアログボックスが表示されます。
- ここで入力するユーザー名、パスワードは、Rooster-VMⅡの設定ツールにアクセスするためのもので、プロバイダから提供されるユーザー名、パスワードとは異なるものです。
  （パスワードの変更方法は、☞3.3 ログインパスワードの設定をご覧ください。）

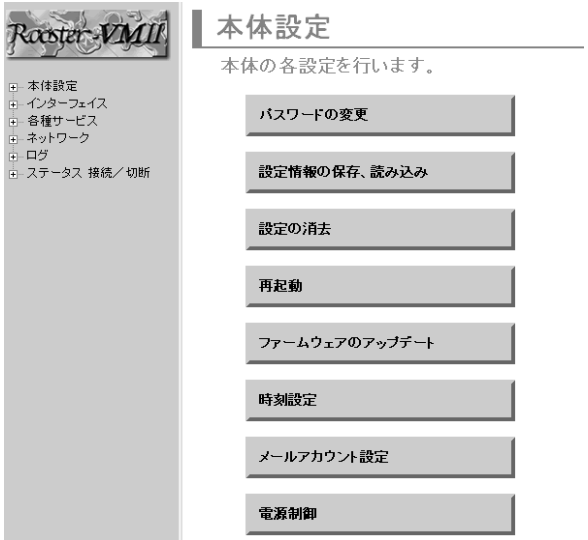


図 3-3　Rooster-VMⅡ Web 設定ツール

3.2　LAN側の設定

Rooster-VMⅡのLAN側IPアドレスを変更する場合に設定を行います。
工場出荷時状態のLAN側IPアドレスは「192.168.62.1」に設定されています。

1. 設定ツールのメニューから、[インターフェイス]－[LAN]をクリックします。
「LAN側設定」のページが表示されます。

図 3-4　LAN 側設定画面

2. [IP アドレス]、[サブネットマスク]に、新しく設定する Rooster-VMⅡの LAN 側 IP アドレス、サブネットマスクを入力します。
3. RIP によるダイナミックルーティングに対応させる場合、「RIP 機能を使用する」のチェックをオンにします。
4. 設定 ボタンをクリックして、設定を反映させます。

> **注意** IP アドレス変更後は、一旦ブラウザを閉じてしばらくお待ちください。その後、新しく設定した IP アドレスで再度設定ツールにログインします。
>
> なお、変更前と異なるサブネットの IP アドレスに変更した場合、
> （例.192.168.62.1⇒192.168.0.1 に変更）
> Rooster-VMⅡ、パソコン共に再起動を行ってください。
> また 192.168.63.0/24 の IP アドレスはメンテナンスポートで使用しているため、設定しましても正常に動作いたしません。

LAN内の通信状態は、設定ツールのメニューから、[ステータス 接続／切断]－[LAN]をクリックして表示される「LANステータス表示画面」から確認することができます。

図 3-5　LAN ステータス表示画面

■ **MAC アドレス**

Rooster-VMⅡのMACアドレスが表示されます。

■ **IP アドレス**

Rooster-VMⅡのIPアドレスが表示されます。

■ **サブネットマスク**

Rooster-VMⅡのサブネットマスクが表示されます。

■ **ステータス(LAN1～4)**

LANポート1～4へのLAN接続機器の接続状態が表示されます。

■ **送信バイト数**

Rooster-VMⅡから送信したデータの総バイト数が表示されます。

■ **送信パケット数**

Rooster-VMⅡから送信したデータの総パケット数が表示されます。

■ **送信エラー回数**

Rooster-VMⅡからデータ送信を行った際に発生したエラー回数の総計が表示されます。

■ **受信バイト数**

Rooster-VMⅡで受信したデータの総バイト数が表示されます。

■ **受信パケット数**

Rooster-VMⅡで受信したデータの総パケット数が表示されます。

■ **受信エラー回数**

Rooster-VMⅡがデータ受信を行った際に発生したエラー回数の総計が表示されます。

3.3 ログインパスワードの設定

ログインパスワードを変更する場合に設定を行います。
工場出荷時状態のパスワードは「1234」に設定されています。

1. 設定ツールのメニューから、[本体設定]－[パスワード変更]をクリックします。
「パスワードの変更」ページが表示されます。

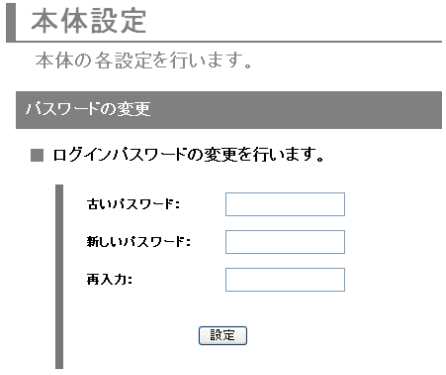


図 3-6　パスワード変更画面

2. [古いパスワード]に、現在使用しているパスワードを入力します。
3. [新しいパスワード]に、新しく設定するパスワードを入力します。
4. [再入力]に、[新しいパスワード]に入力したパスワードを再度入力します。
5. 設定 ボタンをクリックして、設定を反映させます。
6. ログインダイアログボックスが表示されます。新しく設定したパスワードで再度ログインします。

注意
- 入力したパスワードはすべて、「＊」で表示されます。
- 入力可能な文字数は、半角英数字、記号で 16 文字までです。
- ユーザー名の変更はできません。"admin"のみとなります。

3.4 時刻の設定

メモ ここで設定される時刻は、Rooster-VMⅡのログ表示などに使用されます。(ログ表示の詳細は、☞ 10ログの参照方法をご覧ください。)

設定ツールのメニューから、[本体設定]－[時刻設定] をクリックします。
「時刻設定」ページが表示されます。

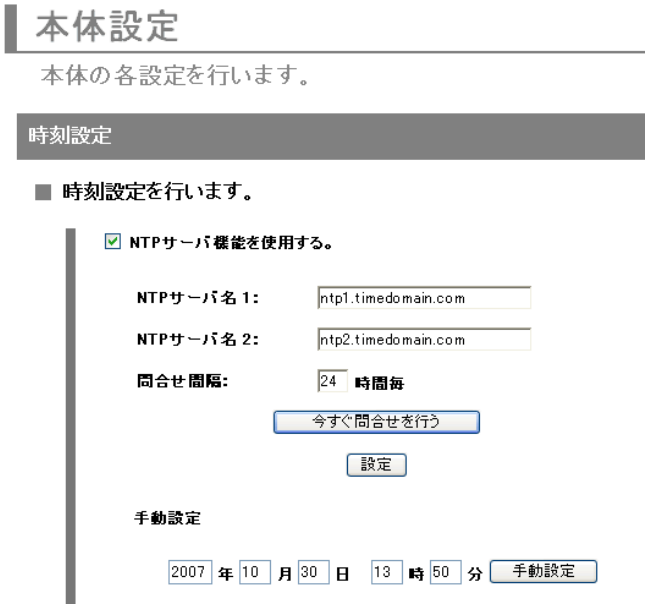


図 3-7　時刻設定画面

3.4.1 NTPサーバを使用して定期的に時刻を同期する場合

> **注意** この機能を使用するには、インターネットに接続している必要があります。（☞インターネット接続設定の詳細は、4.2ダイヤルアップ接続設定をご覧ください。）

1. 「NTP サーバ機能を使用する。」チェックをオンにし、以下の設定を行います。

■ **NTP サーバ名 1**

時刻を問い合わせるNTPサーバアドレス1を入力します。

■ **NTP サーバ名 2**

時刻を問い合わせるNTPサーバアドレス2を入力します。

■ **問合せ間隔**

指定された間隔でサーバにNTPサーバに接続し、時刻を同期します。
“0”を設定した場合、起動後1回のみ実行します。

2. 設定 ボタンをクリックして、設定を反映させます。

設定完了後、今すぐ問合せを行う ボタンをクリックすると、設定したNTPサーバに接続して時刻を同期します。

> **注意** NTP 問い合わせに失敗した場合は、成功するまで約 5 分間隔で問い合わせを実行します。

3.4.2 手動で時刻の設定を行う場合

1. [手動設定]の各欄に、現在の時刻を入力します。
2. 手動設定 ボタンをクリックします。直ちに設定した時刻に調整されます。

> **注意** 時刻同期を行う際、WAN回線が接続されていない場合、モバイルカードの設定（☞4.2ダイヤルアップ接続設定をご覧ください。）によっては自動的にダイヤルを行います。

3.5 メールアカウントの設定

> **メモ** ここで設定されるメールアカウントは、Rooster-VMⅡの、メール送信によるアドレス解決機能（機能の詳細は、☞ 7.1アドレス解決機能をご覧ください。）に使用されます。
>
> メール送信によるアドレス解決機能を使用する必要がない場合、メールアカウントの設定の必要はありません。

1. 設定ツールのメニューから、[本体設定]－[メールアカウント設定] をクリックします。

「メールアカウントの設定」ページが表示されます。

図 3-8 メールアカウント設定画面

2. 以下の設定を行います。

■ **サービスの種類**

メールサーバの種類を選択します。
「POP Before SMTP」、「ユーザ認証 SMTP」のいずれかを選んでください。

■ **SMTP サーバ名**

送信メールサーバ名を設定します。
サーバ名の後に“:ポート番号”を追加することにより、SMTPサーバに接続するポート番号を指定できます。
例）smtp.mailserver.com:587

■ **POP サーバ名**

受信メールサーバ名を設定します。

■ **アカウント**

アカウント名を設定します。

■ **パスワード**

使用するメールアカウントのパスワードを入力します。

> **注意** 上記の設定で不明な部分につきましては、インターネットプロバイダ、あるいはサーバ管理者までお問い合わせください。

3. 設定 ボタンをクリックして、設定を反映させます。

3.6 電源制御

> **メモ** Rooster-VMⅡの電源の制御を行います。この機能は定期的にRooster-VMⅡの電源を OFF/ON することにより、より安定した運用を行うことを目的とします。

1. 設定ツールのメニューから、[本体設定]－[電源制御] をクリックします。
「電源制御」のページが表示されます。

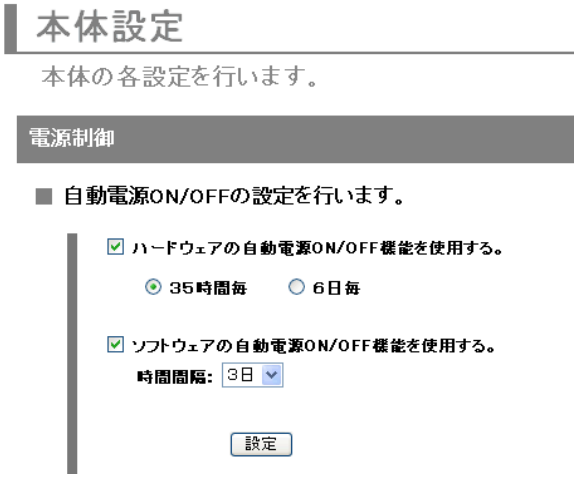


図 3-9 電源制御設定画面

2. 以下の設定を行います。

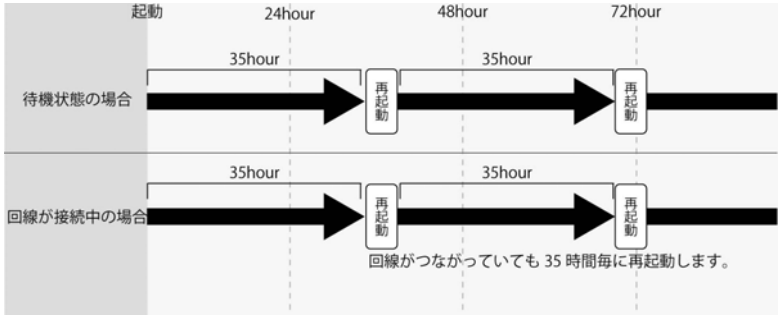
■ **ハードウェア**

ハードウェア上でRooster-VMⅡ本体の電源をOFF/ONさせるための設定です。
使用する場合はチェックを入れ、「35時間毎」、「6日毎」のいずれかを選択します。

> **メモ** ソフトウェアの設定が何等かの影響にて動作しなかった時の保険的な機能です。
>
> ハードウェアの設定時間が目安ですので、実際の動作時間は多少前後します。

> **注意** 回線がつながっている状態でも、設定時間になるとハードウェアが再起動します、

<例>
ハードウェア：35時間毎

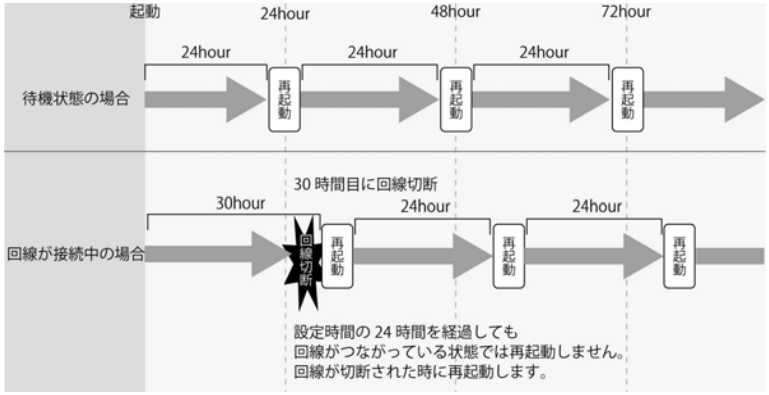


■ **ソフトウェア**

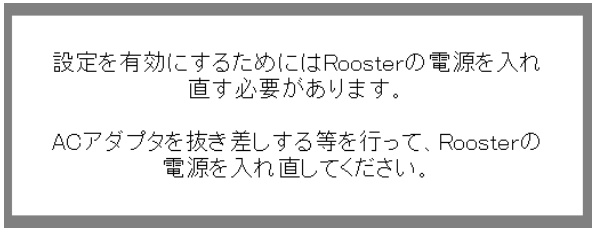
ソフトウェア上でRooster-VMⅡ本体の電源をOFF/ONさせるための設定です。
使用する場合はチェックを入れ、「時間間隔」にリセットさせる間隔を選択してください。

> **注意** 設定時間時に回線がつながっている状態では、ソフトウェアは再起動いたしません。
>
> 回線切断後に再起動します。

<例>
ソフトウェア：使用する、1日毎



3. 選択した設定でよければ 設定 ボタンをクリックします。
4. 設定を反映させるためには、Rooster-VMⅡの電源を入れ直す必要があります。AC アダプタを抜き差しする等を行ってください。



メモ モバイルカードについては、24 時間毎にリセットする機能が搭載されています。回線がつながっている状態ではモバイルカードは再起動せず、回線切断後に再起動します。

4. ダイヤルアップ設定

4.1 プロバイダ情報の確認

インターネット接続の設定を行う場合は、以下のインターネットサービスプロバイダ（以下プロバイダ）等から提供された情報を用意してください。
☞ 2.2ご利用環境の確認をご覧ください。

- **アクセスポイントへの電話番号**
  （料金コースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。）
- **ユーザー名**
- **パスワード**

4.2 ダイヤルアップ接続設定

1. 設定ツールのメニューから、[インターフェイス]－[モバイルカード]－[ダイヤルアップ] をクリックします。

「ダイヤルアップ接続設定」のページが表示されます。

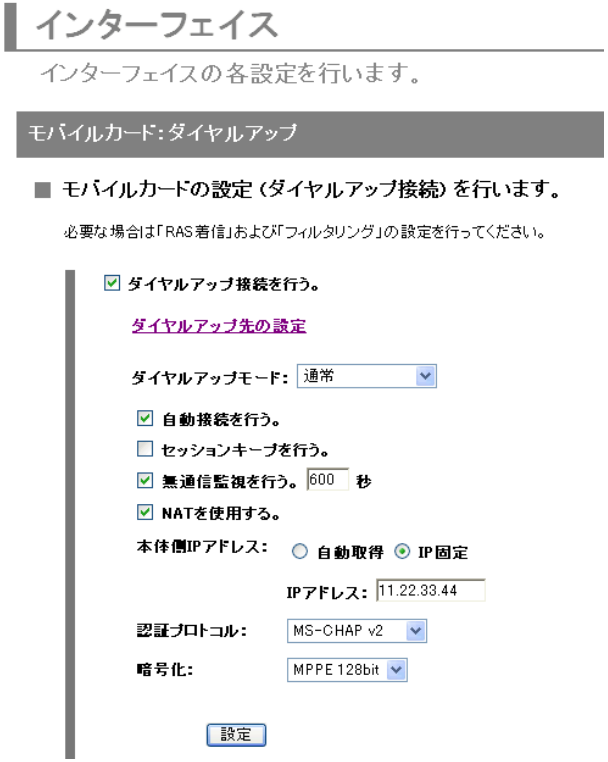


図 4-1　ダイヤルアップ接続設定画面

2. 「ダイヤルアップ接続を行う。」のチェックをオンにし、以下の設定を行います。

注意 必要な場合は「RAS着信」(☞ 5.1 RAS着信接続設定)および「フィルタリング」(☞ 8.3 フィルタリング)の設定を行ってください。

■ **ダイヤルアップ先の設定**

クリックすると、モバイルカードによるダイヤルアップ接続先の表示、追加が行えます。
(設定方法は、☞ 4.2.1 ダイヤルアップ接続先の追加、変更方法をご覧ください。)

■ **ダイヤルアップモードの設定**

ダイヤルアップのモードを選択します。
「通常」、「対向通信」、「ビジネスmopera」、「unnumbered」のいずれかを選択します。

- モードが「通常」の場合

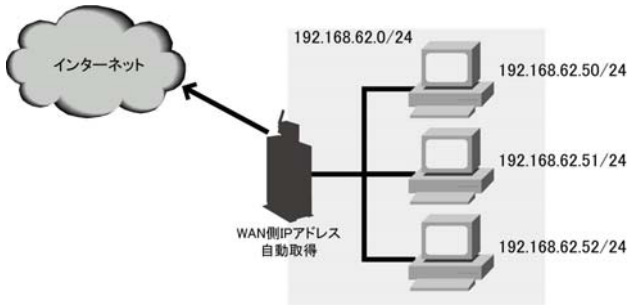


図 4-2 モード「通常」での接続例

インターネットへ接続される場合には「通常」を選択ください。
WAN側のIPアドレスが固定の場合には「本体側IPアドレス」に、指定のIPアドレスを入力してください。

- モードが「対向通信」の場合

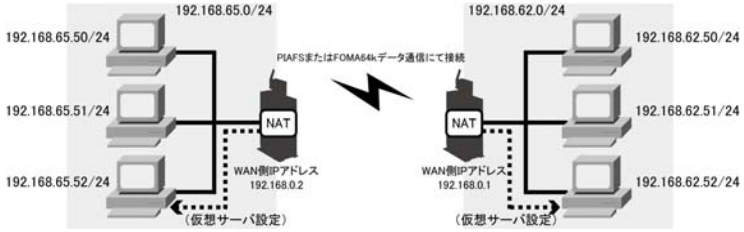


図 4-3 モード「対向通信」で「NAT 使用する」場合の接続例

NATを使用する場合は、仮想サーバもしくはDMZの設定が必要となります。
設定につきましては☞ 8.4 バーチャルサーバまたは☞ 8.5 DMZをご覧ください。

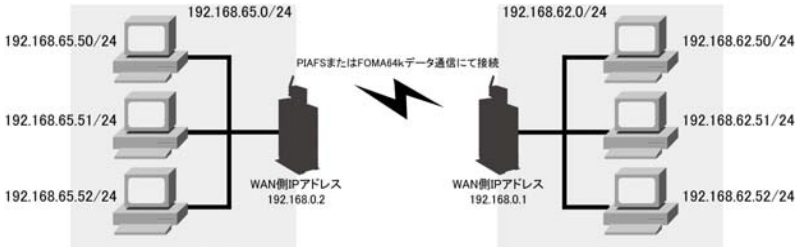


図 4-4 モード「対向通信」で「NAT 使用しない」場合の接続例

NATを使用しない場合は、お互いのLAN側のIPアドレスでの通信が可能になります。

- モードが「ビジネス mopera」の場合

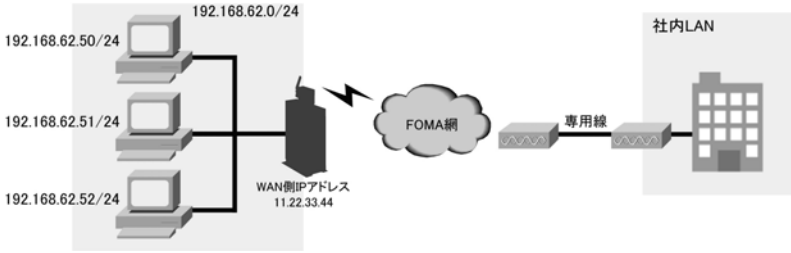


図 4-5 モード「ビジネス mopera」での接続例

NTTドコモのビジネスmoperaアクセスプレミアムをご利用の際には、「ビジネスmopera」を選択ください。

注意 NTTドコモとの契約が必要になります。

ビジネス mopera アクセスプレミアムにつきましては、NTT ドコモのホームページをご覧ください。

● モードが「Unnumbered」の場合

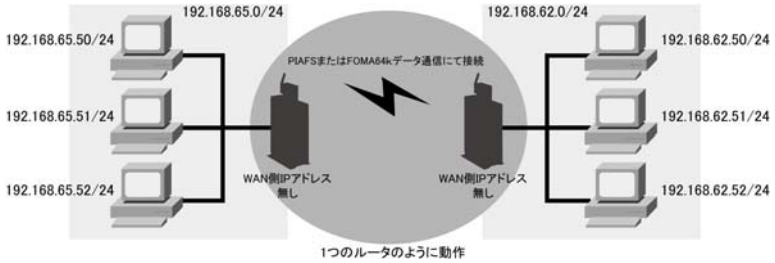


図 4-6　モード「Unnumbered」での接続例

Unnumbered接続とは、他のネットワークに接続するルータのWAN側ポートにIPアドレスを割り当てず、2台のルータを見かけ上1台のルータのように扱う接続方式です。このようにWAN側にIPアドレスを付与せず接続する場合には「Unnumbered」を選択ください。

■ **自動接続を行う**

チェックをオンにすると、LAN側から発信要求があった場合、もしくはRooster-VMⅡの各種サービスによる接続要求があった場合等に、自動発信が行われるようになります。
セッションキープの設定は、自動接続の設定をオンにするとできるようになります。
チェックをオフにすると、接続、切断の動作は設定ツールのみで行うようになります。

■ **セッションキープを行う**

回線接続を維持させておきたい時にチェックをオンにします。

> **注意** 従量制課金でご契約の場合は、設定しないようにしてください。
> **意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。**

■ **無通信監視を行う**

チェックをオンにすると、Rooster-VMⅡが指定した秒数の間、通信が行われなかった時、自動的に回線を切断するようになります。
チェックがオンになっていても、“0”を入力した場合、無通信監視は行いません。

> **注意** 従量制課金でご契約の場合は、必ず設定するようにしてください。

■ **NAT を使用する**

WAN側への通信を行う際にIPアドレスの変換が必要になる場合、チェックをオンにします。
インターネット接続を行う場合、通常はチェックをオンにしてください。

■ **本体側 IP アドレス:自動取得**

WAN側のIPアドレスが自動取得の場合はこちらを選択します。

■ **本体側 IP アドレス:IP 固定**

WAN側のIPアドレスが固定の場合はこちらを選択します。

■ **IP アドレス**

本体側IPアドレスを「IP固定」で選択した際には、IPアドレスを入力します。

> **注意** 「ダイヤルアップモード」の設定で、「対向通信」を選択した場合は、IPアドレスをRooster-VMⅡのLAN側IPとは別のネットワークIPアドレスを指定ください。またIPアドレスは「RAS着信接続」で設定したクライアントIPアドレスと合わせてください。設定方法につきましては☞ 5.1 RAS着信接続設定をご覧ください。

■ **認証プロトコル**

ダイヤルアップの認証プロトコルを選択します。
「相手に合わせる」または「MS-CHAPv2」のどちらかを選択します。
「MS-CHAPv2」を選択した場合、暗号化の設定が有効になります。

■ **暗号化**

暗号化の設定を選択します。
「無効」または「MPPE128bit」のどちらかを選択します。

3. 設定 ボタンをクリックして、設定内容を反映させます。

> **注意** 「ダイヤルアップ先の設定」を行う前に、ここで一度、設定 ボタンをクリックして、設定内容を反映させます。
> **先にクリックすると、設定した内容が破棄されてしまいます。**

4.2.1　ダイヤルアップ接続先の追加、変更方法

1. 「ダイヤルアップ先の設定」をクリックします。
「ダイヤルアップ接続先リスト」のページが表示されます。

図 4-7　ダイヤルアップ接続先リスト画面

2. 新しく接続先の登録を行う場合は、追加 ボタンをクリックします。設定済みのダイヤルアップ接続先を変更する場合は、[変更]をクリックします。
戻る ボタンをクリックすると、「ダイヤルアップ接続設定」のページに戻ります。

3. 追加 ボタン、または[変更]をクリックすると、「ダイヤルアップ接続先の詳細設定」ページが表示されます。
   追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、「ダイヤルアップ接続先の詳細設定」ページが表示され、表示されている接続先設定の変更が行えます。
   [削除]をクリックすると、表示されている接続先設定が削除されます。
   戻る ボタンをクリックすると、「ダイヤルアップ接続設定画面」のページに戻ります。

> **注意** 設定可能な接続先は 1 件のみです。

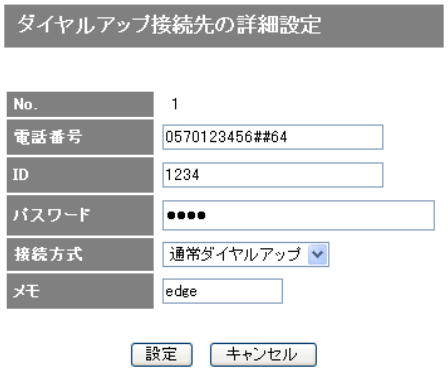


図 4-8　ダイヤルアップ接続先設定画面

4. 以下の設定を行います。

■ **電話番号**

アクセスポイントへの電話番号を入力します。
電話番号の-(ハイフン)は、入力してもしなくても構いません。
電話番号設定の詳細は、☞ 4.4.1 インターネット接続の料金コースと専用通信方式、および☞ 4.4.2 PIAFS通信方式をご覧ください。

> **注意** アクセスポイントへの電話番号は、料金コースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。

■ **ID**

プロバイダから提供されたユーザー名を入力します。

■ **パスワード**

プロバイダから提供されたパスワードを入力します。

> **注意** 上記の設定でご不明な部分につきましては、インターネットプロバイダ、あるいはサーバ管理者までお問い合わせください。

■ **接続方式**

「通常ダイヤルアップ」のみの設定となります。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

5. 設定 ボタンをクリックして設定内容を反映させます。
   キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「ダイヤルアップ接続先リスト」のページに戻ります。

4.3　接続/切断方法

1. 設定ツールのメニューから、[ステータス]－[モバイルカード] をクリックします。
   「モバイルカード通信ステータス」のページが表示されます。

図 4-9　モバイルカードステータス表示画面(接続完了状態)

■ **ステータス（ダイヤルアップ接続時）**

設定したダイヤルアップ接続の現在の状態が表示されます。
[詳細表示]をクリックすると、現在の状態をより詳しく参照できます。

表 4-1　モバイルカードのステータス一覧

ステータス表示	状態	本体 Mobile ランプの状態	
		緑	橙
無効	接続設定が無効になっています。	消灯	消灯
未装備	カードが挿入されていないか、カードが認識できていません。	消灯	消灯
使用しない	カードは正常に認識されていますが、接続設定が行われていません。	消灯	消灯
待受中	カードが正常に認識されていて、接続設定も行われていますが、接続が行われていない状態です。	消灯	消灯
ダイヤルアップ発信中	接続先へ電話を掛け始めた状態です。	消灯	点滅
ダイヤルアップ PPP ネゴ中	プロバイダ(RAS サーバ)で認証を行っている状態です。	点灯	点滅
ダイヤルアップ接続完了	接続が正常に行えた状態です。	点灯	点灯

注意 電源を入れた状態でカードの抜き差しを行うと、モバイルカードが挿入されていても、ステータスが "未装備" となる場合があります。この場合、Rooster-VMⅡの再起動を行ってください。
またカードの抜き差しは、必ず電源を切った状態で行ってください。

■ **接続先**

設定した接続先電話番号が表示されます。

■ **操作**

それぞれ以下の操作を行います。

- [接続]⇒接続動作を行います。
- [切断]⇒切断動作を行います。
- [無効]⇒設定を無効にします。
  次回、[有効]をクリックするまで設定内容を使えないようにします。
- [有効]⇒設定を有効にします。
  次回、[無効]になっている設定を再度使えるようにします。

4.3.1　通信ステータス詳細表示

図 4-10　モバイルカード通信ステータス詳細表示画面

■ **ステータス**

設定したダイヤルアップ接続の現在の状態が表示されます。

■ **電話番号**

設定したアクセスポイントへの電話番号が表示されます。

■ **ユーザー名**

設定したユーザー名が表示されます。

■ **IP アドレス**

プロバイダおよび接続先から割り当てられた、Rooster-VMⅡのWAN側IPアドレスが表示されます。

■ **ゲートウェイ**

ゲートウェイのIPアドレスが表示されます。

■ **DNS サーバ 1**

DNSサーバ1のIPアドレスが表示されます。

■ **DNS サーバ 2**

DNSサーバ2のIPアドレスが表示されます。

■ **送信バイト数**

モバイルカード通信で送信したデータの総バイト数が表示されます。

■ **送信パケット数**

モバイルカード通信で送信したデータの総パケット数が表示されます。

■ **送信エラー回数**

モバイルカードでデータ送信を行った際に発生した、エラー回数の総計が表示されます。

■ **受信バイト数**

モバイルカード通信で受信したデータの総バイト数が表示されます。

■ **受信パケット数**

モバイルカード通信で受信したデータの総パケット数が表示されます。

■ **受信エラー回数**

モバイルカードでデータ受信を行った際に発生した、エラー回数の総計が表示されます。

メモ ダイヤルアップ接続が正常に行えない場合、本体ランプの点灯状況、およびステータス、ログなどから、その原因の切り分けを行うことができます。

ステータス、本体ランプの点灯状況は、☞ 4.3接続/切断方法を、ログ表示の詳細は、☞ 10ログの参照方法をご覧ください。

4.4 対応通信モード一覧

4.4.1 インターネット接続の料金コースと専用通信方式

通信業者	ご利用の料金コース	通信方式の名称	電話番号の形式
（株）ウィルコム	つなぎ放題 [8×]、[4×]	PRO/8×/4x パケット方式	〈電話番号〉##64
	つなぎ放題 [1×]	1x パケット方式	〈電話番号〉##61
	ネット 25 [8×]、[4×]	PRO/8×/4x パケット方式	〈電話番号〉##64
	ネット 25	フレックスチェンジ方式	〈電話番号〉##7
エヌ・ティ・ティドコモ	FOMA	384k パケット通信	注 1) ＊99＊＊＊●#
		64k 回線交換	＊9601
KDDI（株）	CDMA 1X WIN	3.6M パケット通信	＊99＊＊24#
ソフトバンクモバイル（株）	アクセスインターネット	3.6M パケット通信	＊99#
		64k 回線交換	＊7300

注1)●は、APNの設定で登録を行ったcid番号（1-10）が入ります。
（moperaでは初期値は ”1” 、moperaUでは初期値は ”3”となります。）
mopera以外の登録を行う場合は、FOMAカードの取扱説明書等をご覧ください。

4.4.2　PIAFS通信方式

通信業者	通信方式	電話番号の形式
（株）ウィルコム	PIAFS 32k	〈電話番号〉##3
	PIAFS 64k	〈電話番号〉##4

注意

- 電話番号の設定は、必ず接続先、通信方式をご確認の上、正しく設定を行うようにしてください。
  定額制でのご契約でも、専用の接続先、通信方式以外で通信を行った場合、基本料金とは別に通信料金が発生します。
- パケット通信方式は、パケット通信で接続可能なプロバイダの場合のみ使用できます。
  それ以外の場合は、回線交換方式で接続を行います。
- パソコンにモバイルカードのドライバをインストールする必要はありません。Rooster-VMⅡが自動認識します。
  ただし、モバイルカードに付属のユーティリティソフトは、Rooster-VMⅡ経由では動作致しません。
- モバイルカードのサービスエリア外（圏外）では使用できません。(モバイルカードの表示ランプを確認してください。)
- モバイルカードのサービスエリア内でも、電波の受信状況が悪い場合、回線が混んでいる場合などには、通信が不安定になることもあります。
- データ圧縮機能への対応は以下の通りです。
  - 対応

    NTTドコモのネットハイウェイサービス
  - 未対応

    （株）ウィルコムのAIR-EDGE MEGA PLUS

    『Venturi Client』がLAN経由でのインターネット接続に対応致しておりません。

5.　着信設定

5.1　RAS着信接続設定

メモ　RAS 着信機能について

RAS（Remote Access Service）とは、電話回線を通じて遠隔地のネットワークにダイヤルアップ接続し、そのネットワークの資源を利用する機能をいいます。

1. 設定ツールのメニューから、[インターフェイス]－[モバイルカード]－[RAS 着信] をクリックします。

「RAS着信」設定のページが表示されます。

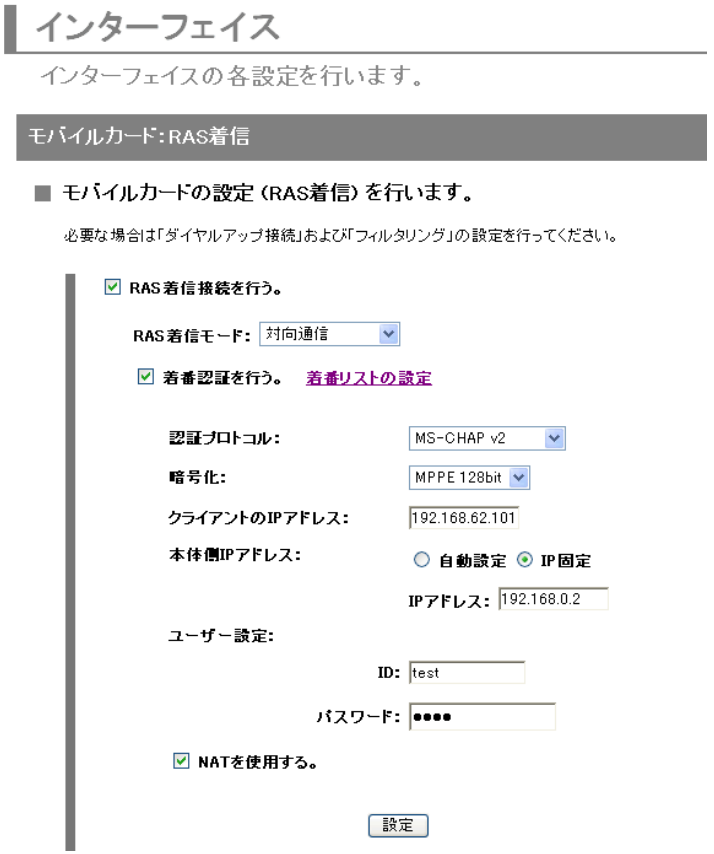


図 5-1　RAS 着信設定画面

2. 「RAS 着信接続を行う。」チェックをオンにし、以下の設定を行います。

注意 必要な場合は「ダイヤルアップ接続（☞ 4.2ダイヤルアップ接続設定）および「フィルタリング」（☞ 8.3フィルタリング）の設定を行ってください。

■ **RAS 着信モード**

RAS着信モードを選択します。
「通常」、「対向通信」、「ビジネスmopera」、「Unnumbered」のいずれかを選択します。

- モードが「通常」の場合

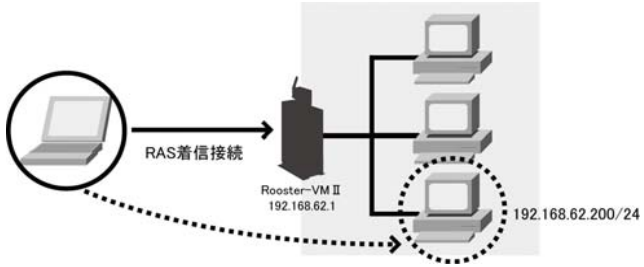


図 5-2 モードが「通常」の場合の接続

外部からアクセスしたパソコンのIPアドレスはRooster-VM ⅡのLAN側のIPアドレスとなります。

- モードが「対向通信」の場合

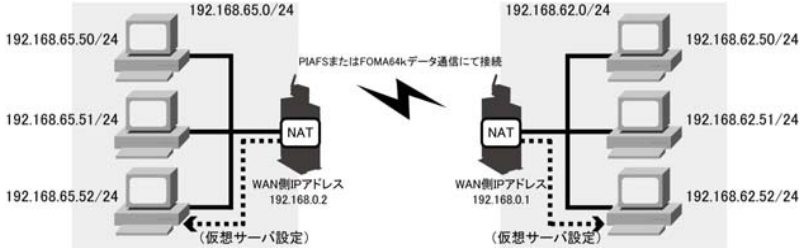


図 5-3 モード「対向通信」で「NAT 使用する」場合の接続例

NATを使用する場合は、仮想サーバもしくはDMZの設定が必要となります。
設定につきましては☞ 8.4 バーチャルサーバまたは☞ 8.5 DMZをご覧ください。

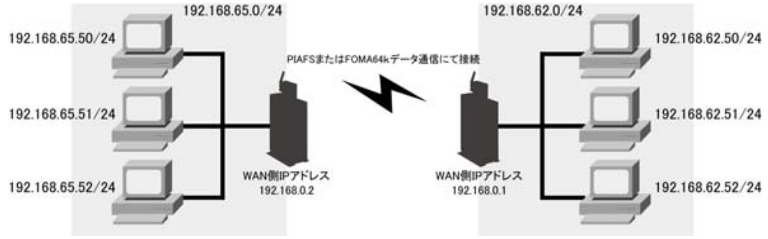


図 5-4 モード「対向通信」で「NAT 使用しない」場合の接続例

NATを使用しない場合は、お互いのLAN側のIPアドレスでの通信が可能になります。

- モードが「ビジネス mopera」の場合

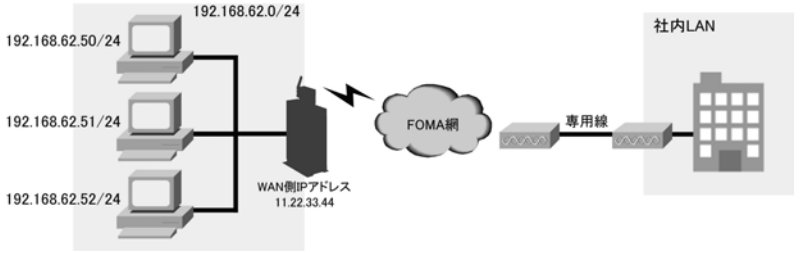


図 5-5 モード「ビジネス mopera」での接続例

NTTドコモのビジネスmoperaアクセスプレミアムのIP着信オプションをご利用の際には、「ビジネスmopera」を選択ください。

注意 NTT ドコモとの契約が必要になります。

ビジネス mopera アクセスプレミアムにつきましては、NTT ドコモのホームページをご覧ください。

- モードが「Unnumbered」の場合

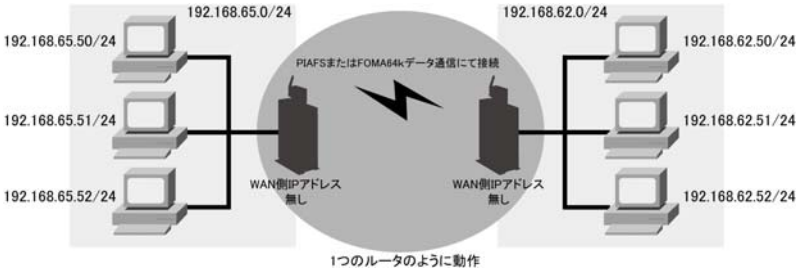


図 5-6　モード「Unnumbered」での接続例

Unnumbered接続とは、他のネットワークに接続するルータのWAN側ポートにIPアドレスを割り当てず、2台のルータを見かけ上1台のルータのように扱う接続方式です。このようにWAN側にIPアドレスを付与せず接続する場合には「Unnumbered」を選択ください。

■ **着番認証を行う**

相手先の電話番号でも認証を行いたい場合、チェックをオンにします。
オンにすると、「着番リストの設定」へのリンク(☞ 5.1.1 着信番号での認証設定をご覧ください。) が有効となります。

■ **認証プロトコル**

認証の際に使用するプロトコルを選択します。
「CHAP」、「PAP」、「相手に合わせる」、「MS-CHAPv2」のいずれかを設定します。
「MS-CHAPv2」を選択した場合、暗号化の設定が有効になります。

注意 RAS 着信モードを「通常」で選択した場合、認証プロトコルは「CHAP」または「PAP」でのみ接続が可能となります。

■ **暗号化**

暗号化の設定を選択します。
「無効」または「MPPE128bit」のどちらかを選択します。

■ **クライアントの IP アドレス**

RAS着信でログインを行ったクライアントに割り当てるIPアドレスを設定します。

注意 クライアントの IP アドレスの設定について

「RAS 着信モード」で「通常」を選択した場合は以下の条件を満たすものを設定してください。

- Rooster-VM Ⅱ の LAN IP アドレスと同じネットワーク内の IP アドレス。
- DHCP サーバ機能をオンにしている場合、その割り当てられる範囲以外の IP アドレス。

「RAS 着信モード」で「対向通信」を選択した場合は以下の条件を満たす IP アドレスを設定してください。

- LAN 側のネットワークとは別のネットワーク IP アドレスを設定してください。
- 「ダイヤルアップ接続」の設定で、「本体側の IP アドレス」で設定した IP アドレスと同じネットワークアドレスを設定してください。

■ **本体側 IP アドレス:自動取得**

WAN側のIPアドレスが自動取得の場合はこちらを選択します。

■ **本体側 IP アドレス:IP 固定**

「RAS着信モード」で「対向通信」または「ビジネスmopera」を選択した場合、本体側のIPアドレスを固定にて設定する場合に選択ください。

■ **IP アドレス**

本体側IPアドレスを「IP固定」で選択した際には、IPアドレスを入力します。

注意 「RAS 着信モード」で「対向通信」を選択した場合には、「クライアント IP アドレス」で設定した IP アドレスと同じネットワークアドレスを入力ください。

例:クライアント IP アドレス:192.168.100.1
　本体側 IP アドレス:192.168.100.2

■ **ユーザー設定**

認証に使用するユーザー名、パスワードを入力します。

■ **NAT を使用する**

「RAS着信モード」で「通常」以外を選択した場合、必要に応じて設定してください。

3. 設定 ボタンをクリックします。

注意 引き続いて「着信番号での認証設定」も行う場合は、ここで一度、設定 ボタンをクリックして、設定内容を反映させます。
先にクリックすると、設定した内容が破棄されてしまいます。

5.1.1 着信番号での認証設定

Rooster-VM Ⅱでは、ユーザ名、パスワードによる認証と同時に、発信者電話番号による認証を行うことも可能です。

1. 「着番リストの設定」をクリックします。

「RAS着信相手先リスト」のページが表示されます。

図 5-7 RAS 着信相手先リスト画面

2. RAS 着信相手先の追加を行いたい場合は、追加 ボタンをクリックします。RAS 着信相手先を変更する場合は、[変更]をクリックします。
（戻る ボタンをクリックすると、「RAS 着信」設定のページに戻ります。）

> **メモ** 着信相手先の設定は最大 50 件まで行えます。

「RAS着信相手先の詳細設定」ページが表示されます。

図 5-8 RAS 着信相手先設定画面

3. 以下の設定を行います。

■ 電話番号

RAS着信相手先の電話番号を入力します。
電話番号のハイフンは入力してもしなくても構いません。

■ メモ

設定内容を分かりやすくするための覚え書きを入力します。16文字までの任意の文字列を入力できます。

4. 設定 ボタンをクリックし、設定内容を反映させます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

5.1.2 RAS着信時のステータス表示

1. 設定ツールのメニューから[ステータス]－[モバイルカード]をクリックします。
「モバイルカード通信ステータス」のページが表示されます。

図 5-9 モバイルカードステータス表示画面(着信接続完了状態)

■ **ステータス（RAS 着信時）**

設定したRAS着信の現在の状態が表示されます。
[詳細表示]をクリックすると、現在の状態をより詳しく参照できます。

表 5-1　モバイルカードのステータス一覧

ステータス表示	状態	本体 Mobile ランプの状態	
		緑	橙
無効	接続設定が無効になっています。	消灯	消灯
未装備	カードが挿入されていないか、カードが認識できていません。	消灯	消灯
使用しない	カードは正常に認識されていますが、接続設定が行われていません。	消灯	消灯
待受中	カードが正常に認識されていて、接続設定も行われていますが、接続が行われていない状態です。	消灯	消灯
着信接続中	遠隔地からの接続機器のアクセスを確認した状態です。	消灯	点滅
着信 PPP ネゴ中	Rooster-VMⅡで、接続機器の認証を行っている状態です。	点灯	点滅
着信接続完了	着信接続が正常に行えた状態です。	点灯	点灯

注意 電源を入れた状態でカードの抜き差しを行うと、モバイルカードが挿入されていても、ステータスが "未装備" となる場合があります。この場合、Rooster-VMⅡの再起動を行ってください。
またカードの抜き差しは、必ず電源を切った状態で行ってください。

注意
- RAS着信はモバイルカードログに記録されます。
（ログ表示の詳細は、☞10.2.1モバイルカードログをご覧ください。）
- RAS着信で使用可能なモバイルカードは、対応する一部のモバイルカードのみとなります。対応するモバイルカードは、弊社ホームページの対応機種一覧をご覧ください。
http://www.sun-denshi.co.jp/sc/rooster_vm2/card.html

5.2　ダイヤルアップ接続設定とRAS着信設定の併用

Rooster-VMⅡでは、ダイヤルアップ接続設定とRAS着信を併用させることが可能です。
待受中に着信があった場合は、RAS着信の設定が有効になり、着信動作を行います。
逆に待受中に接続要求があった場合は、ダイヤルアップ接続の設定が有効となり、ダイヤルアップ動作を行います。

- ダイヤルアップ接続設定は、☞ 4 ダイヤルアップ設定をご覧ください。
- RAS着信接続設定は、☞ 5.1 RAS着信接続設定をご覧ください。

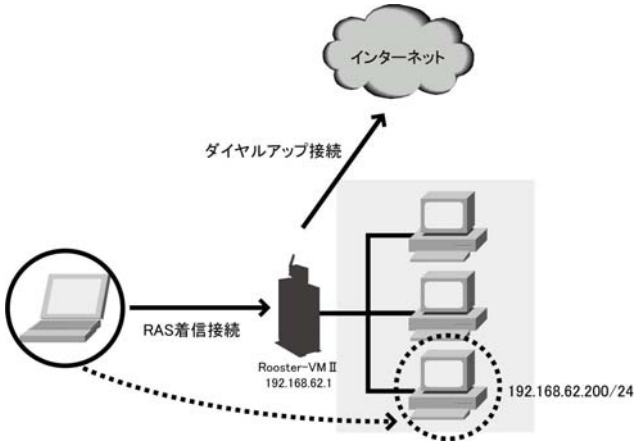


図 5-10　ダイヤルアップ接続と RAS 着信接続

注意
- RAS 着信接続と排他使用となります。
(同時に接続することはできません。)
- ダイヤルアップ接続の各設定と RAS 接続の各設定は独立していますので、それぞれ設定してください。

5.3 WakeOn着信設定

メモ WakeOn 着信について

待ち受け状態のモバイルカードを、遠隔地からの操作によりダイヤルアップさせることを可能とする機能です。

KDDI(株)のセンタープッシュサービス、(株)ウィルコムの WakeOn サービスに対応しています。

また AIR EDGE 端末によるライトメール、および携帯電話等からによる音声着信にも対応しています。

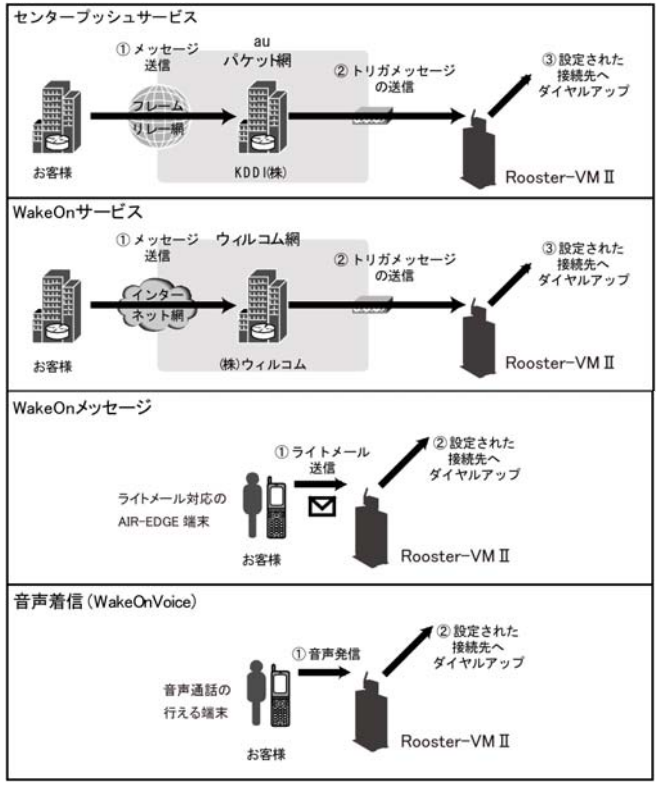


図 5-11 WakeOn 着信機能の概要

1. 設定ツールのメニューから、[インターフェイス]－[モバイルカード]－[WakeOn 着信] をクリックします。

「モバイルカード:WakeOn着信」設定のページが表示されます。

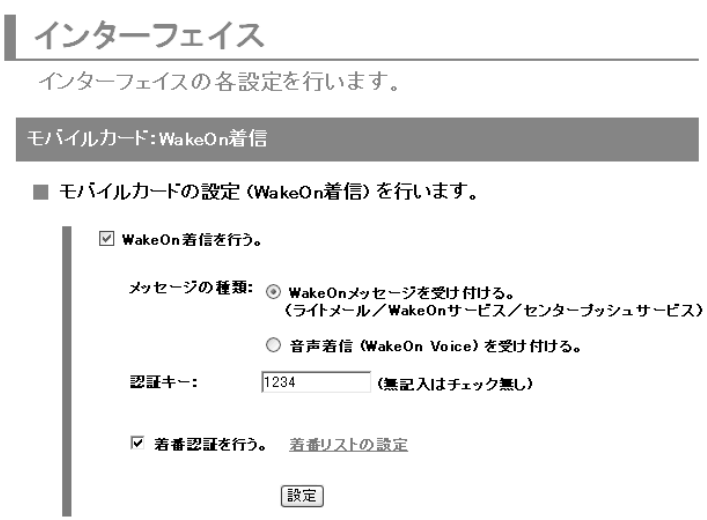


図 5-12 WakeOn 着信設定画面

2. 「WakeOn 着信を行う。」チェックをオンにし、以下の設定を行います。

■ **WakeOn メッセージを受け付ける。**

WakeOnメッセージを受信してWakeOn着信を行う場合は、こちらを選択します。

■ **音声着信(WakeOn Voice)を受け付ける。**

音声着信を受信してWakeOn着信を行う場合は、こちらを選択します。

■ **認証キー**

WakeOnメッセージの文字列による認証を行えます。
「WakeOnメッセージを受け付ける。」設定を有効にした時に設定できます。
認証キーは、(受信したメッセージの先頭文字)～(設定された認証キー文字数)までを比較し、一致した場合は成功となります。
ただし、一文字でも異なった場合は認証失敗となります。
なお空白の場合、認証は行いません。認証キーは半角英数字のみです。

表 5-2 WakeOn メッセージ認証設定例

設定した認証キー	受信したメッセージ	結果	
1234	5678	×	全く一致していないため
1234	1234	○	全文字一致しているため
12	1234	○	先頭 2 文字が一致しているため
12345	1234	×	5 文字目が一致しないため

■ **着番認証を行う**

WakeOnを行う発信端末を限定させたい場合、チェックをオンにすると、発信者電話番号で認証を行うことができます。
オンにすると「着番リストの設定」へのリンクが有効となります。

3. 設定 ボタンをクリックして、設定内容を反映させます。

> **注意** 引き続いて「着番リストの設定」も行う場合は、ここで一度、設定 ボタンをクリックして、設定内容を反映させます。
> **先にクリックすると、設定した内容が破棄されてしまいます。**

5.3.1 着信番号での認証設定

1. 「着番リストの設定」をクリックします。

「WakeOn着信相手先リスト」のページが表示されます。

図 5-13 WakeOn 着信リスト画面

2. WakeOn 着信リストの追加を行いたい場合は、追加 ボタンをクリックします。設定済みの WakeOn 着信相手先を変更する場合は、[変更]をクリックします。
戻る ボタンをクリックすると、「WakeOn 着信設定画面」のページに戻ります。

追加 ボタンまたは、[変更]をクリックすると、「WakeOn着信リストの詳細設定」ページが表示されます。
追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。
[削除]をクリックすると、表示されているWakeOn着信リスト設定が削除されます。

> **メモ** 着信リストの設定は最大 16 件まで行えます。

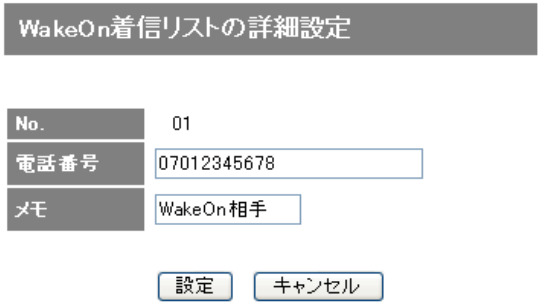


図 5-14 WakeOn 着信設定画面

3. 以下の設定を行います。

■ **電話番号**

WakeOn着信相手先の電話番号を入力します。
電話番号の－(ハイフン)は、入力してもしなくても構いません。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字（全角8文字）までの任意の文字列を入力できます。

4. 設定 ボタンをクリックし、設定内容を反映させます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「WakeOn 着信相手先リスト」のページに戻ります。

> **注意**
> - センタープッシュのサービスを利用する場合は、KDDI(株)との契約が必要です。
> - WakeOn サービスを利用する場合は、(株)ウィルコムとの契約が必要です。

> **注意**
> - WakeOn着信による発信は、モバイルカードログに記録されます。
> (ログ表示の詳細は、☞10.2.1 モバイルカードログをご覧ください。)
> - 音声着信(WakeOn Voice)の場合、電話を掛ける端末は、発信者番号通知、および音声発信が行える端末で可能ですが、Rooster-VM Ⅱ側で使用可能なモバイルカードは、対応する一部のモバイルカードのみとなります。対応するモバイルカードは、弊社ホームページの対応機種一覧をご覧ください。
> http://www.sun-denshi.co.jp/sc/rooster_vm2/card.html

6. Rooster-VMⅡ メンテナンス

6.1 設定情報の保存、読み込み

設定ツールのメニューから、[本体設定]－[設定情報の保存、読み込み] をクリックします。
「設定情報の保存、読み込み」のページが表示されます。

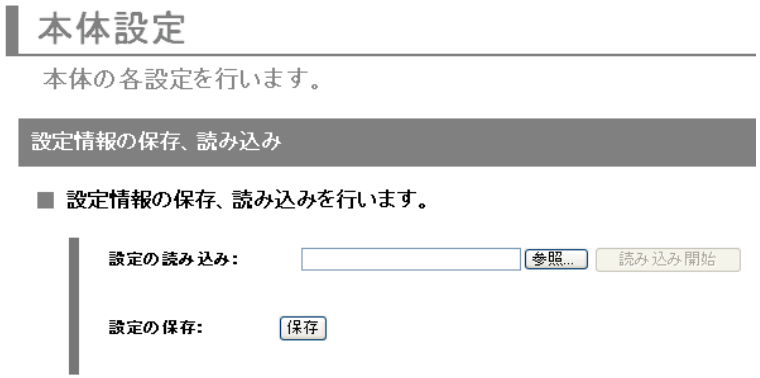


図 6-1 設定情報保存、読み込み画面

6.1.1 現在の設定を保存

[現在の設定]テキストボックス内の設定情報の保存を行います。

1. [設定の保存]の 保存 ボタンをクリックします。
「rooster.cfg」がダウンロードされます。

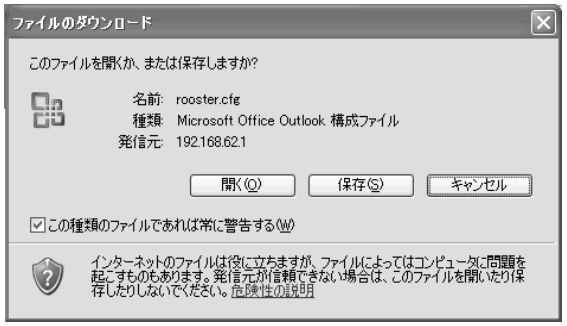


図 6-2 コンフィグファイルのダウンロード（Windows SP2 の場合）

2. 保存(S) ボタンをクリックし、「rooster.cfg」の保存先を指定します。
Rooster-VMⅡの設定情報が、指定した保存先にダウンロードされます。

6.1.2 保存した設定の読み込み

1. [設定の読み込み]の 参照 ボタンをクリックし、読み込みを行う設定情報ファイル「*.cfg」のある場所を指定します。
2. 読み込み開始 ボタンをクリックします。
Rooster-VMⅡの設定が保存時の設定に書き戻されます。

6.2 設定情報の消去

1. 設定ツールのメニューから、[本体設定]－[設定の消去] をクリックします。
「設定の消去」のページが表示されます。

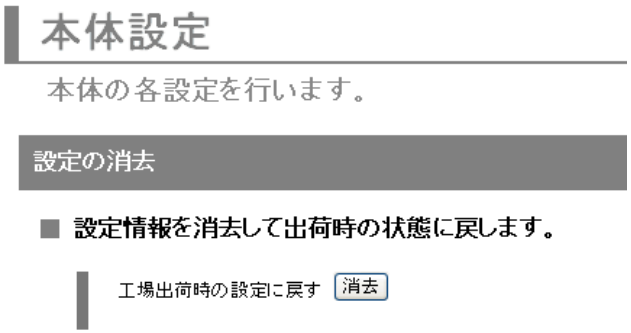


図 6-3 設定情報消去画面

2. [工場出荷時の設定に戻す]の 消去 ボタンをクリックします。
確認ダイアログで[OK]をクリックすると、Rooster-VMⅡが再起動し、設定が工場出荷時の状態にリセットされます。

注意 設定情報の初期化は、Rooster-VMⅡ本体にあるリセットスイッチの長押しでも行うことができます。

その方法は、☞ 1.4 各部の名称と機能をご覧ください。

6.3 ファームウェアのアップデート方法

メモ アップデートファイルは、新しいモバイルカードへの対応、機能追加、プログラム修正などが行われるたびに、弊社ホームページにて随時公開を行う予定です。

下記の手順を行う前に、以下のページよりファームウェアのイメージファイルをダウンロードしてください。

Rooster-VMⅡ製品情報

http://www.sun-denshi.co.jp/sc/rooster_vm2/

1. 設定ツールのメニューから、[本体設定]－[ファームウェアアップデート] をクリックします。「ファームウェアのアップデート」ページが表示されます。

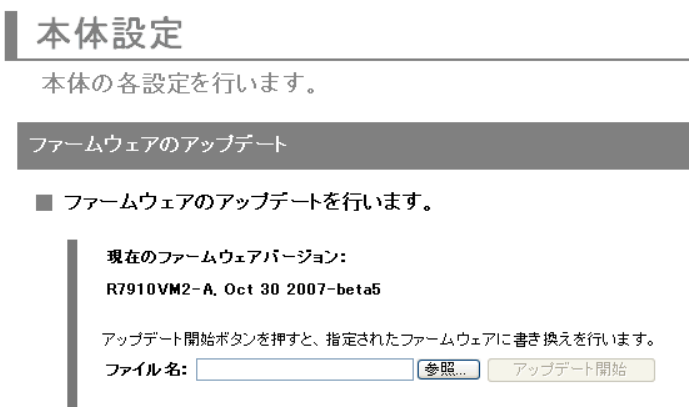


図 6-4　ファームウェアアップデート画面

2. 参照 ボタンをクリックして、ダウンロードしたアップデートプログラムデータ「*.img」のある場所を指定します。
3. アップデート開始 ボタンをクリックします。

確認ダイアログで[OK]をクリックすると、Rooster-VMⅡのファームウェアがアップデートされます。

> **注意** アップデートを実行すると、SNMP機能を使用している場合強制停止されます。SNMP機能の詳細につきましては、☞ 7.7 SNMPをご覧ください。

> **警告** ファームウェアのアップデートが完了するまで、4～5 分程度かかります。**アップデート中は、背面の AC アダプタを絶対に抜かないようにしてください。動作不能となる恐れがあります。**
>
> これにより動作不能となった場合、有償修理となりますのでご注意願います。

6.4 Rooster-VMⅡの再起動

1. 設定ツールのメニューから、[本体設定]－[再起動] をクリックします。

「再起動」ページが表示されます。

図 6-5　再起動画面

2. 再起動 ボタンをクリックします。

> **注意** 再起動が完了するまで、2 分程度かかります。

6.5 メンテナンスポート

Rooster-VMⅡには、管理者が設定を行うようにするための、「メンテナンスポート」が用意されています。LANポートからRooster-VMⅡへのアクセスを許可しない設定にすると、設定はメンテナンスポートからのみ可能となります。
メンテナンスポートの使用方法は以下の通りです。

- 接続機器の方に固定 IP アドレスを指定する必要があります。
  ネットワークは、192.168.63.0/24 となります。
  (〈例〉接続機器の IP アドレス:192.168.63.10、サブネットマスク:255.255.255.0)
- メンテナンスポートから Rooster-VMⅡの Web 設定画面へログインする場合、「http://192.168.63.1」へアクセスを行います。
  メンテナンスポートの IP アドレス設定は、192.168.63.1 です。
- ログインパスワードは LAN ポートと共通です。
- Webサービス機能で、「LANポートからのアクセスを許可する。」のチェックを外すと、(設定の詳細は、☞ 7.5 Webサービスをご覧ください。)LANポートから設定ツールにログインできないようにさせることができます。
- TELNETログインについても、同様に行うことができます。
  (設定の詳細は、☞ 7.4 TELNETサービスをご覧ください。)
- メンテナンスポートからは、LAN ポート、および WAN へは一切ルーティングされません。

> **注意** LAN ポートから Rooster-VMⅡへアクセスを許可しないように設定しても、ping やインターネット接続など、その他の通信には影響しません。

7. 各種サービス設定

7.1 アドレス解決機能

メモ アドレス解決機能について

外部ネットワークから、インターネットに接続された Rooster-VM Ⅱにアクセスする場合、Rooster-VM Ⅱに割り当てられたグローバル IP アドレスの情報が必要になりますが、通常のインターネット接続ではインターネットに接続するたびに、グローバル IP アドレスは任意に変化します。

Rooster-VM Ⅱでは、変化するグローバル IP アドレスを指定メールアカウントに通知する機能、ダイナミック DNS サーバを利用する機能のいずれかの方法によって、上記問題を解決することができます。

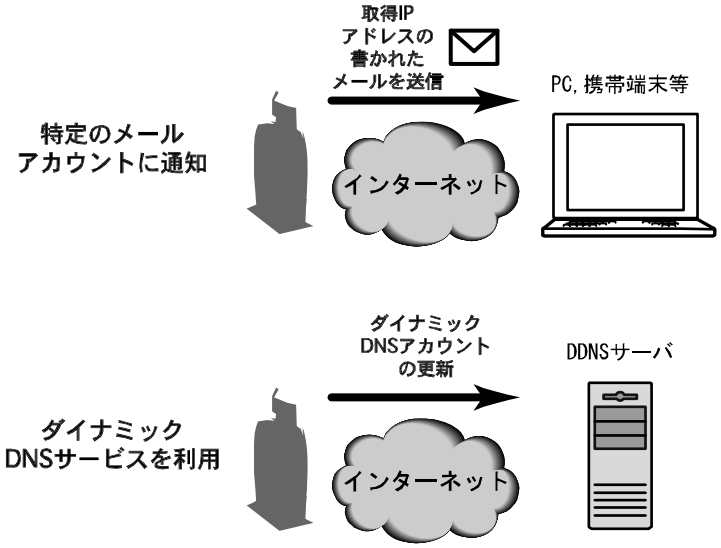


図 7-1 アドレス解決機能の概要

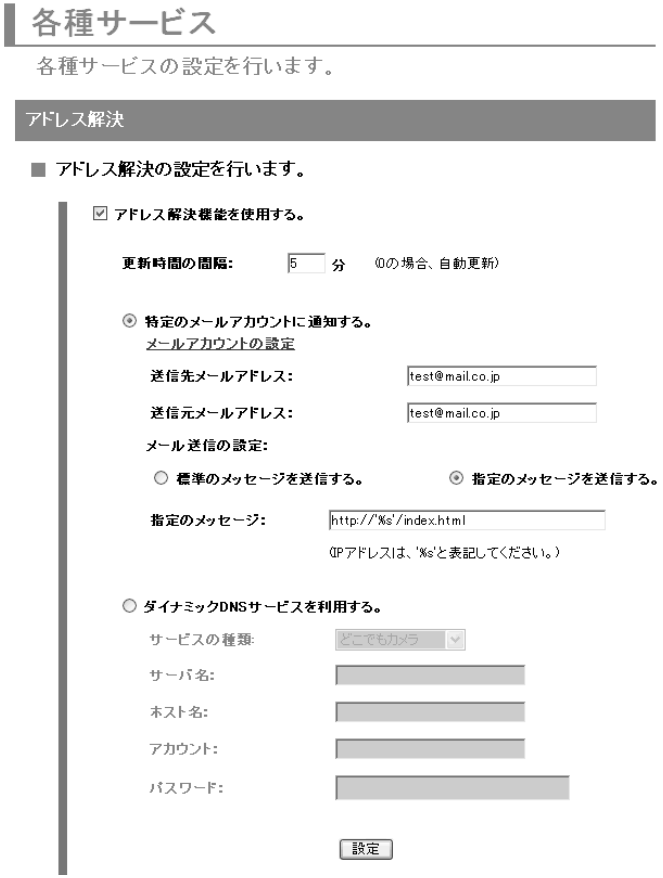


図 7-2 アドレス解決機能設定画面

設定ツールのメニューから、[各種サービス]－[アドレス解決]をクリックします。「アドレス解決」設定のページが表示されます。
アドレス解決機能を使用する場合は、「アドレス解決機能を使用する。」チェックをオンにし、以下の設定を行います。

7.1.1 IPアドレスを指定メールアカウントに通知する設定

1. 「特定のメールアカウントに通知する。」のチェックをオンにし、以下の設定を行います。

■ **更新時間の間隔**

指定メールアカウントに、設定された時間ごとにメール送信します。"0"を設定した場合自動更新となり、グローバルIPアドレスが変更された時のみ、メール送信を行います。
"0"以外を設定される場合、設定の最小値は5(分)となります。

■ **メールアカウントの設定**

（設定方法は☞ 3.5 メールアカウントの設定をご覧ください。）

注意 引き続いて「メールアカウントの設定」も行う場合は、ここで一度 設定 ボタンをクリックして、設定内容を反映させます。
先にクリックすると、設定した内容が破棄されます。

■ **送信先メールアドレス**

グローバルIPアドレスを通知させたいメールアドレスを入力します。

■ **送信元メールアドレス**

送信者のメールアドレスを入力します。

注意 送信元メールアドレスの入力がないと、メールサーバによってはメールが送信されない場合があります。

■ **メール送信の設定**

通知メールのメッセージ内容を指定したい場合は、「指定のメッセージを送信する。」を選択します。必要がなければ、「標準のメッセージを送信する。」を選択します。
標準のメッセージは、以下のような形式で送信されます。

☞**送信メールの例**

```
タイトル:Rooster IP Report
送信者:Rooster(004053010203)　⇒カッコ内は Rooster-VMⅡの MAC アドレス
内　容:Rooster IP-Address Report v0.01.
　　MAC=004053010203　　⇒Rooster-VMⅡのMACアドレス
　　IP=10.20.30.40　　⇒割り当てられるグローバルIPアドレス
```

文字列を指定して入力を行う場合、指定のメッセージ入力フォームに、"%s" ("は不要)と入力すると、取得したグローバルIPアドレスに変換されて通知されます。
例)割り当てグローバルIPアドレスが"11.22.33.44"の場合。

設定内容	実際に送信されるメッセージ
http://%s/mobile	http://11.22.33.44/mobile

2. 設定 ボタンをクリックして、設定内容を反映させます。

7.1.2　ダイナミックDNSサーバを利用する設定

1. 「ダイナミック DNS サービスを利用する。」のチェックをオンにし、以下の設定を行います。

■ **更新時間の間隔**

指定されたダイナミックDNSサービスへ、設定された時間ごとに更新を行います。
"0"を設定した場合自動更新となり、グローバルIPアドレスが変更された時のみ、ダイナミックDNSサービスへの更新を行います。
0以外を設定される場合、設定の最小値は5(分)となります。

■ **サービスの種類**

アドレス解決に使用するダイナミックDNSサービスを選択します。
「どこでもカメラ」、「DynDns.org」、「SunComm.DDNS」のいずれかを設定します。

注意 ダイナミック DNS サービスを使用される場合は、別途契約または登録が必要となります。詳細につきましては、下記の URL をご覧ください。

- **「どこでもカメラ」**

  ヴィ･インターネットオペレーションズ(株)
  http://www.vio.co.jp/

- **「DynDns.com」**

  Dynamic DNS Network Services
  http://www.dyndns.com/
  DynDNS.orgサービスは、できる限り試用でのみお使いいただくことをお勧めします。
  長期間におよぶ運用用途でご使用の場合は、十分に動作検証を行ってください。恐れ入りますが、弊社ではこの場合の動作保証および責任につきましては一切負いかねます。ご了承願います。

- **「suncomm.DDNS」**

  http://www.sun-denshi.co.jp/sc/ddns/index.html
  弊社が運用する有償でのダイナミックDNSサービスです。
  別途、ご契約が必要となりますので、上記URLをご参照ください。
  また、「suncomm.DDNS」機能を利用して、お客様独自にダイナミックDNSサーバを設置・運用いただくことも可能です。
  「suncomm.DDNS」のプロトコル仕様につきましては、機密保持契約成立後、開示させていただきます。なお、本件は法人のお客様に限らせていただきます。

- 「どこでもカメラ」を選択した場合
  [サーバ名]、[ホスト名]、[アカウント]、[パスワード]を入力します。
- 「DynDns.org」を選択した場合
  [ホスト名]、[アカウント]、[パスワード]を入力します。
- 「SunComm.DDNS」を選択した場合
  [サーバ名]、[ホスト名]、[アカウント]、[パスワード]を入力します。

2. 設定 ボタンをクリックして、設定内容を反映させます。

7.2 DNSサービス

1. 設定ツールのメニューから、[各種サービス]－[DNS サービス]をクリックします。
   「DNSサービス」設定のページが表示されます。

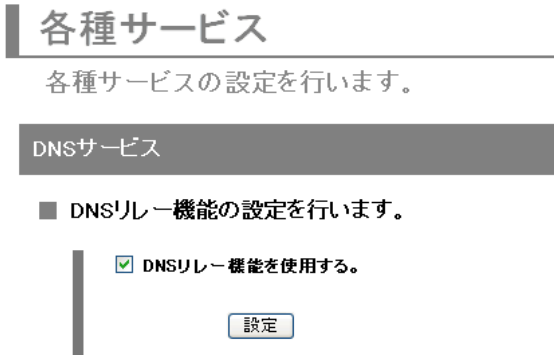


図 7-3　DNS サービス設定画面

2. DNS リレー機能を使用する場合、「DNS リレー機能を使用する。」チェックをオンにします。
3. 設定 ボタンをクリックして、設定内容を反映させます。

- DNS リレー機能を使用するかしないかによって、接続機器 TCP/IP 設定の DNS サーバ設定方法が異なってきます。以下のうち該当する設定を行ってください。

DNS リレー機能を使用する場合。

⇒下記のいずれかの設定を行います。

- DNS サーバアドレスを自動的に取得するように設定します。
- DNS サーバアドレスを指定する場合、Rooster-VMⅡの LAN IP アドレス、またはプロバイダ指定の DNS サーバ（ネームサーバ）アドレスを指定します。

DNS リレー機能を使用しない設定の場合。

⇒自動取得されないので、指定する必要があります。
プロバイダ指定のDNSサーバ（ネームサーバ）アドレスを指定します。

7.3 DHCPサービス

1. 設定ツールのメニューから、[各種サービス]－[DHCP サービス]をクリックします。
   「DHCPサービス」設定のページが表示されます。

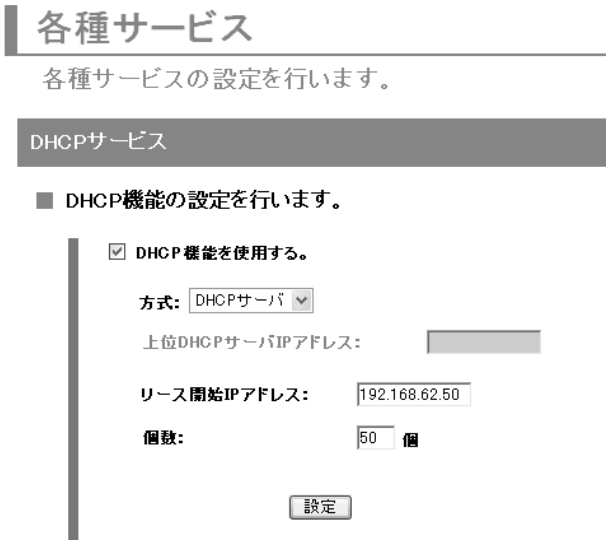


図 7-4　DHCP サービス設定画面

2. DHCP 機能を使用する場合、「DHCP 機能を使用する。」チェックをオンにします。
3. DHCP 機能の[方式]として「DHCP サーバ」、「DHCP リレー」のいずれかを選択します。

■ 「DHCP サーバ」を選択した場合

Rooster-VMⅡ自身をDHCPサーバとして動作させたい場合に設定します。
[リース開始IPアドレス]に、割り当てるIPアドレスの開始アドレスを入力します。[個数]に、DHCPサーバ機能で使用する、リース開始IPアドレスからのアドレスの個数を指定します。
初期設定では、[リース開始IPアドレス]が「192.168.62.50」、[個数]が「50」と設定されているので、「192.168.62.50～192.168.62.99」が、DHCPサーバ機能で使用するIPアドレスの範囲となります。

■ 「DHCP リレー」を選択した場合

Rooster-VMⅡ以外の機器をDHCPサーバとして動作させたい場合に設定します。
[上位DHCPサーバIPアドレス]に、DHCPサーバとして動作させる機器のIPアドレスを入力します。

4. 設定 ボタンをクリックして、設定内容を反映させます。

Rooster-VMⅡのDHCPテーブルは、設定ツールのメニューから、[ステータス 接続／切断]－[DHCP割り当て一覧]をクリックして表示される「DHCP割り当て表示画面」から確認することができます。

図 7-5　DHCP 割り当て表示画面

■ **IP アドレス**

Rooster-VMⅡ LAN内にあるLAN接続機器に割り当てたIPアドレスが表示されます。

■ **MAC アドレス**

上記のIPアドレスを付与された、LAN接続機器のMACアドレスが表示されます。

注意 Rooster-VMⅡを再起動すると、DHCP テーブルはすべてリセットされます。

再起動後、クライアントからの IP アドレス割り当て要求を受けたタイミングで、再度 DHCP テーブルに登録されます。

7.4　TELNETサービス

メモ
- TELNET サービスによって、Web 設定ツールで設定可能なすべての項目を設定できます。
（設定ツールで行えない設定も一部可能です。）
- TELNETコマンドの詳細は、同梱 CD-ROM 内の『**TELNET 設定機能説明書**』をご覧ください。

1. 設定ツールのメニューから、[各種サービス]－[TELNET サービス]をクリックします。
「TELNETサービス」設定のページが表示されます。

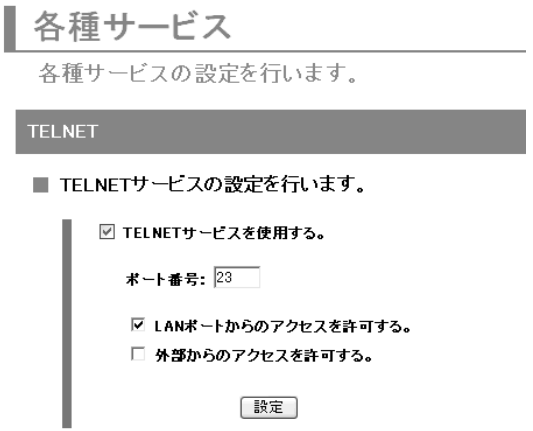


図 7-6　TELNET サービス設定画面

2. TELNET サービスを使用する場合、「TELNET サービスを使用する。」チェックをオンにします。
3. [ポート番号]で、TELNET サービスで使用するポート番号を入力します。
4. 以下の設定を行います。

■ **LAN ポートからのアクセスを許可する。**

チェックをオンにすると、LAN1～4ポート、およびメンテナンスポートからのTELNETログインができます。
オフにすると、メンテナンスポートからのみTELNETログインができます。

■ **外部からのアクセスを許可する。**

チェックをオンにすると、WAN側からのTELNETログインを許可します。
オフにすると、WAN側からのTELNETログインを拒否します。

5. 設定 ボタンをクリックして、設定内容を反映させます。

7.5 Webサービス

メモ Web サービスについて

Web サービスは、Rooster-VMⅡの設定ツールにアクセスを行う機能です。

設定により LAN ポート、WAN、メンテナンスポートのうち、設定ツールにアクセスできるポートを決定することができます。

1. 設定ツールのメニューから、[各種サービス]－[Web サービス]をクリックします。
「Webサービス」設定のページが表示されます。

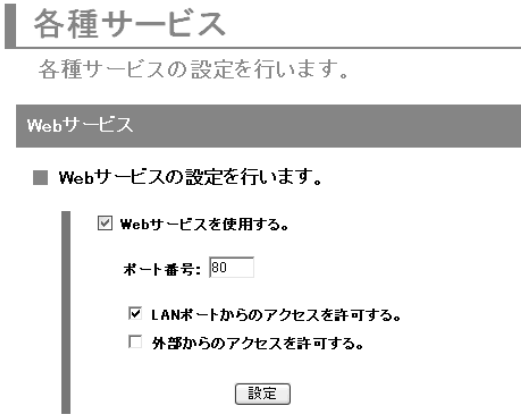


図 7-7 Web サービス設定画面

2. Web サービスを使用する場合、「Web サービスを使用する。」チェックをオンにします。
3. [ポート番号]で、Web サービスで使用するポート番号を入力します。
4. 以下の設定を行います。

■ **LAN ポートからのアクセスを許可する。**

チェックをオンにすると、LAN1～4ポート、およびメンテナンスポートからの設定ツールへのログインができます。
オフにすると、メンテナンスポートからのみ設定ツールへのログインができます。

■ **外部からのアクセスを許可する。**

チェックをオンにすると、WAN側からの設定ツールへのログインを許可します。
オフにすると、WAN側からの設定ツールへのログインを拒否します。

5. 設定 ボタンをクリックして、設定内容を反映させます。

7.6 QoS

メモ QoS 機能について

QoS(Quality of Service)とは、ネットワーク上で、ある特定の通信のための帯域を予約し、一定の通信速度を保証する技術のことをいいます。

Rooster-VMⅡでは、送信元、相手先 IP アドレスとポート番号で通信を特定し、その通信の帯域を確保することができます。

- QoS の設定は、以下の図の○の方向への通信に適用されます。

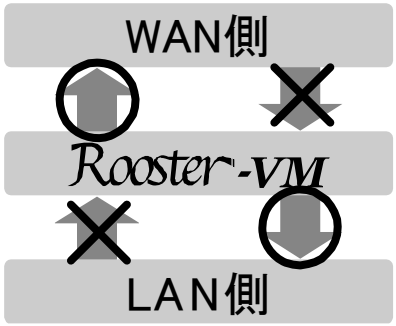


図 7-8 QoS の適用範囲

1. 設定ツールのメニューから、[各種サービス]－[QoS]をクリックします。
「QoS設定リスト」のページが表示されます。

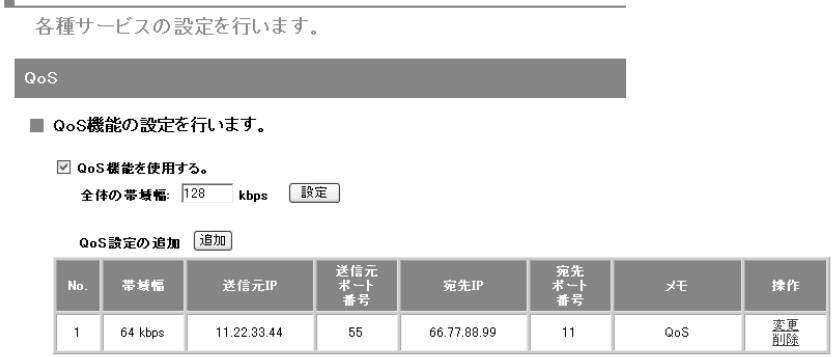


図 7-9 QoS 機能設定画面

2. QoS 機能を使用する場合、「QoS 機能を使用する。」チェックをオンにします。
3. [全体の帯域幅]に、接続を行うサービスの帯域の理論値を入力します。
例）128k パケット通信サービスの場合、”128”と入力します。
4. 設定 ボタンをクリックして、設定内容を反映させます。

> **注意** QoS 機能の追加を行う前に、ここで一度、 設定 ボタンをクリックして、設定内容を反映させます。
> **先に 追加 ボタンをクリックすると、設定した内容が破棄されてしまいます。**

7.6.1 QoS機能の追加設定

1. QoS 機能の追加を行う場合は、 追加 ボタンをクリックします。
   既存の設定を変更する場合は、[変更]をクリックします。

   [削除]をクリックすると、表示されている設定が削除されます。
   追加 ボタンまたは、[変更]をクリックすると、「QoS機能の詳細設定」ページが表示されます。
   追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

> **メモ**
> - QoS 機能の設定は最大 8 件まで行えます。
> - 設定が適用される優先順位は、No の昇順となり、No.1 が一番高い優先順位となります。

図 7-10 QoS 機能詳細設定画面

2. 以下の設定を行います。

■ **No.**

QoS機能設定の通し番号が表示されます。

■ **宛先インターフェイス**

この設定を適用するインターフェイスを選択します。
[LAN] 、[モバイルカード]のいずれかを指定します。

■ **帯域幅**

設定を行う通信に割り当てる帯域を設定します。

■ **送信元 IP**

設定を行う通信の送信元IPアドレスを設定します。
入力がない場合、すべての送信元に設定が適用されます。

■ **送信元ポート番号**

設定を行う通信の送信元ポート番号を設定します。
入力がない場合、すべてのポート番号に設定が適用されます。

■ **宛先 IP**

設定を行う通信の宛先IPアドレスを設定します。
入力がない場合、すべての宛先に設定が適用されます。

■ **宛先ポート番号**

設定を行う通信の宛先ポート番号を設定します。
入力がない場合、すべてのポート番号に設定が適用されます。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

3. 設定 ボタンをクリックすると、「QoS 設定リスト」のページに戻り、設定した内容が反映されます。
   キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

> **注意** QoS 機能は、設定された帯域を必ず保証するものではありません。
> 実回線速度が遅い場合、設定された帯域通りに確保できない場合がございます。

7.7 SNMP

メモ SNMP について

SNMP（Simple Network Management Protocol）は、ネットワーク機器の状態をネットワーク経由で問い合わせたり、それに答えたりするための通信手順の一つをいいます。

SNMP を使用することによって、ネットワーク管理を容易に行うことができるようになります。

SNMP コミュニティは、監視する側のネットワーク監視端末（SNMP マネージャ）と、監視される側のネットワーク上の機器（SNMP エージェント）により構成され、このうち Rooster-VMⅡは、SNMP エージェントとしての動作に対応しております。

対応バージョンは、SNMPv1 のみとなります。

1. 設定ツールのメニューから、[各種サービス]－[SNMP]をクリックします。
「SNMP」設定のページが表示されます。

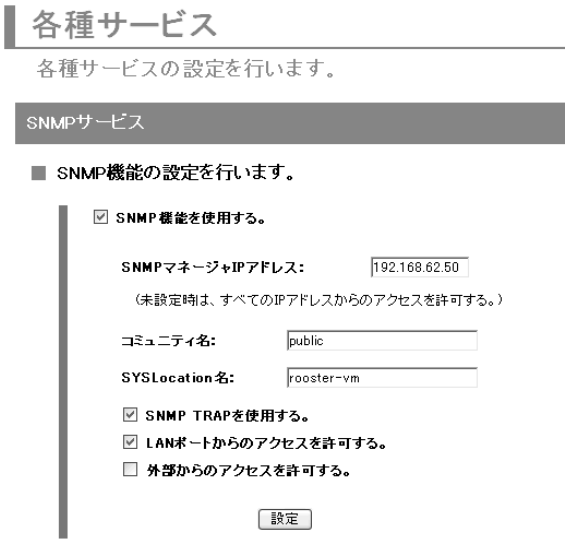


図 7-11　SNMP サービス設定画面

2. SNMP 機能を使用する場合、「SNMP 機能を使用する。」チェックをオンにします。
3. 以下の設定を行います。

■ **SNMP マネージャ IP アドレス**

SNMPマネージャのローカルIPアドレスを設定します。

■ **コミュニティ名**

SNMPマネージャとRooster-VMⅡがやり取りを行うためのコミュニティ名を設定します。
最大16文字まで設定できます。

■ **SYSlocation 名**

MIB変数のSYSLocation名を設定します。

■ **SNMP TRAP を使用する**

Rooster-VMⅡから、SNMPマネージャIPアドレス宛に SNMP TRAPを送信する場合、チェックをオンにします。

■ **LAN ポートからのアクセスを許可する。**

チェックをオンにすると、LAN1～4ポート、およびメンテナンスポートからのアクセスができます。
オフにすると、メンテナンスポートからのみアクセスができます。

■ **外部からのアクセスを許可する。**

チェックをオンにすると、WAN側からのアクセスができます。
オフにすると、WAN側からのアクセスができません。

4. 設定 ボタンをクリックして、設定内容を反映させます。

7.8 WANハートビート機能

メモ WAN ハートビート機能について

WAN ハートビート機能は、WAN 側のネットワークが正常に動いているかどうかの確認を行うための機能です。

1. 設定ツールのメニューから、[各種サービス]－[WAN ハートビート]をクリックします。
「WANハートビート」設定のページが表示されます。

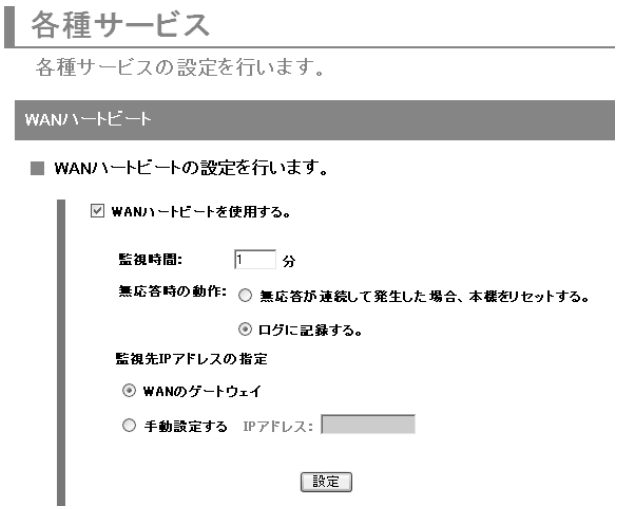


図 7-12 WAN ハートビート設定画面

2. WAN ハートビートを使用する場合、「WAN ハートビートを使用する。」のチェックをオンにします。
3. 以下の設定を行います。

■ **監視時間**

設定された監視間隔でWANハートビートを実行します。
“0”を設定した場合、Rooster-VMⅡ再起動直後のみWANハートビートを実行します。
“0”以外を設定される場合、設定の最小値は1(分)となります。

■ **無応答時の動作**

WANハートビートで、接続状態の確認ができなかった場合に行う動作を選択します。

- **無応答が連続して発生した場合、本機をリセットする。**
10 回連続失敗した時点で、Rooster-VMⅡを再起動します。
- **ログに記録する。**
再起動は行わず、設定された監視時間ごとにWAN ハートビートログに”失敗”のログを記録します。

■ **監視先 IP アドレスの指定**

WANハートビートを行う相手先を指定します。相手先IPアドレスを手動で設定することもできます。

4. 設定 ボタンをクリックして、設定内容を反映させます。

注意

- 従量制課金でご契約の場合は、設定しないようにしてください。
意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。
- WAN 側のゲートウェイ機器の仕様により、WAN ハートビートによる ping に応答しない場合があります。
ping に応答しない場合は手動設定にて IP アドレスを入力するか、無応答時の動作の設定を「WAN ハートビートログを記録する」にご選択ください
- WANハートビート機能は、以下の理由により無通信監視時間（☞ 4.2ダイヤルアップ接続設定をご覧ください）の設定と併用できません。
  - （無通信監視時間）＜（WAN ハートビート監視時間）の場合無通信監視時間で一旦切断されても、WAN ハートビートで再度、自動発信を行ってしまいます。
  - （無通信監視時間）＞（WAN ハートビート監視時間）の場合無通信監視時間で切断される前に、WAN ハートビートの通信により無通信状態がリセットされ、切断されません。

7.9 ログ管理

1. 設定ツールのメニューから、[各種サービス]－[ログ管理]をクリックします。
「ログ管理」設定のページが表示されます。

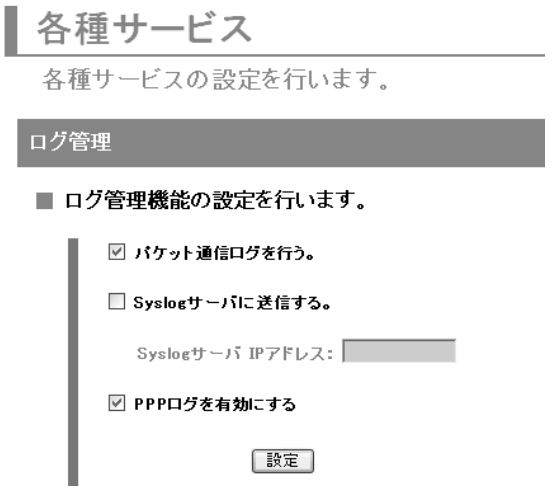


図 7-13 ログ管理機能設定画面

2. 「パケット通信ログを行う。」のチェックをオンにすると、[ログ]－[パケット通信ログ]の[通過ログ]、[遮断ログ]が有効になります。
   パケット通信ログの詳細は、☞ 10.1.1 パケット通過ログまたは☞ 10.1.2 パケット遮断ログをご覧ください。
3. Rooster-VMⅡではなく、Syslog サーバでログ管理を行いたい場合、「Syslog サーバに送信する。」のチェックをオンにし、Syslog サーバのローカル IP アドレスを入力します。この設定を行った場合、Rooster-VMⅡで取得できる全てのログを syslog サーバへ送信します。
4. 「PPPログを行う。」にチェックをオンにすると[ログ]－[サービスログ]の[PPPログ]が有効になります。
   PPPログの詳細は、☞ 10.3.4 PPPログをご覧ください。
5. 設定 ボタンをクリックして、設定内容を反映させます。

8. ネットワーク設定

8.1 VPNパススルー

メモ VPN パススルーについて

VPN パススルーの設定を行うと、Rooster-VMⅡ以外の別の端末が VPN サーバやクライアントとして動作する時、各 VPN プロトコルを通過させることができるようになります。

1. 設定ツールのメニューから、[ネットワーク]－[パススルー]をクリックします。
   「VPNパススルー」設定のページが表示されます。

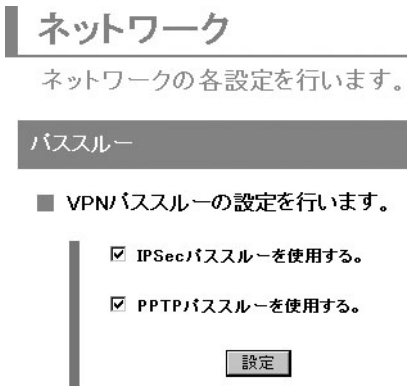


図 8-1 VPN パススルー設定画面

2. 通過させる VPN プロトコルのチェックをオンにします。
3. 設定 ボタンをクリックして、設定内容を反映させます。

8.2 スタティックルーティング

1. 設定ツールのメニューから、[ネットワーク]－[スタティックルーティング]をクリックします。
   「スタティックルーティング」リストのページが表示されます。

図 8-2 スタティックルーティングリスト画面

2. スタティックルートの追加を行いたい場合は、追加 ボタンをクリックします。
   設定済みのスタティックルーティング設定を変更する場合は、[変更]をクリックします。
   [削除]をクリックすると、表示されている設定が削除されます。

   追加 ボタンまたは、[変更]をクリックすると、「スタティックルーティングの詳細設定」ページが表示されます。
   追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ スタティックルートの設定は最大 32 件まで行えます。

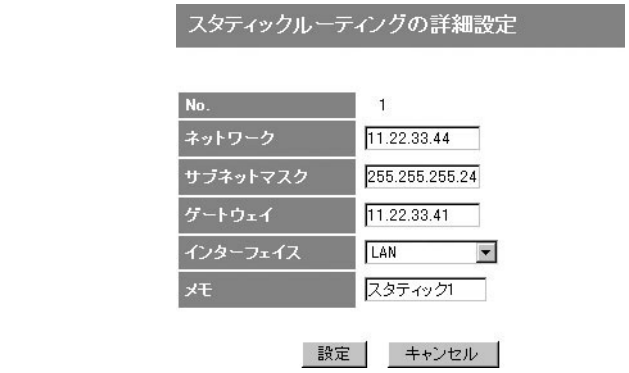


図 8-3 スタティックルーティング詳細設定画面

3. 以下の設定を行います。

■ **ネットワーク**

宛先ネットワークアドレスを入力します。

■ **サブネットマスク**

上記ネットワークのサブネットマスクを入力します。

■ **ゲートウェイ**

上記ネットワークのゲートウェイアドレスを入力します。

■ **インターフェイス**

この設定を適用するインターフェイスを選択します。
[LAN]を指定します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

4. 設定 ボタンをクリックすると、「スタティックルーティングリスト」のページに戻り、設定した内容が反映されます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

8.3 フィルタリング

1. 設定ツールのメニューから、[ネットワーク]－[フィルタリング]をクリックします。
「フィルタリング」リストのページが表示されます。

No.	インターフェイス	方向	動作	プロトコル	宛先IPアドレス	宛先ポート	メモ	操作
1	全て	送信	許可	TCP		80 - 80	HTTP	変更 削除
2	全て	送信	許可	UDP		53 - 53	DNS	変更 削除
3	全て	送信	許可	TCP		25 - 25	SMTP	変更 削除
4	全て	送信	許可	TCP		110 - 110	POP3	変更 削除
5	全て	送信	許可	TCP		1720 - 1720	NetMeeting	変更 削除
6	全て	送信	許可	TCP		1503 - 1503	NetMeeting	変更 削除
7	全て	送信	許可	TCP		443 - 443	SSL	変更 削除
8	全て	送信	許可	ICMP		-	ICMP	変更 削除
9	全て	送信	許可	TCP		21 - 21	FTP	変更 削除

図 8-4　フィルタリング設定リスト画面

2. フィルタリング設定を行った項目以外のパケットをどう処理するかにより、「基本ポリシー」の

■ **「設定されていないパケットはすべて通す。」**
■ **「設定されていないパケットはすべて遮断する。」**

のうちいずれかを選択します。

注意
- 設定済みの項目につきましては、「基本ポリシー」の設定に関わらず、個別に設定した動作が適用されます。
- VPN間の通信は、この設定に関わらず、基本ポリシーは「全て通す」設定で固定となります。
（VPN設定の詳細は、☞ 9 VPN設定をご覧ください）

3. フィルタリング設定追加の追加を行いたい場合は、追加 ボタンをクリックします。
設定済みのフィルタリング設定を変更する場合は、[変更]をクリックします。
[削除]をクリックすると、表示されている設定が削除されます。

追加 ボタンまたは、[変更]をクリックすると、「フィルタリングの詳細設定」ページが表示されます。
追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ フィルタリングの設定は最大 32 件まで行えます。

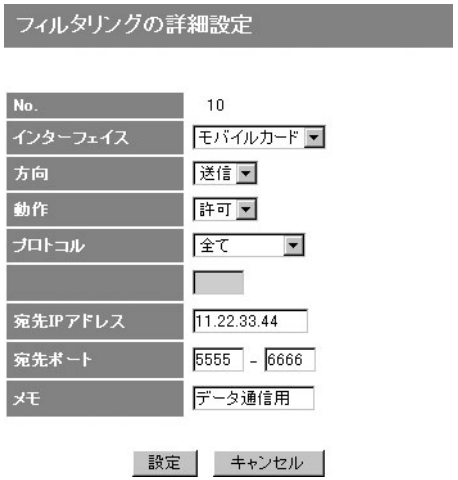


図 8-5　フィルタリング詳細設定画面

4. 以下の設定を行います。

■ **インターフェイス**

この設定を適用するインターフェイスを選択します。
[モバイルカード]、[VPN]、[全て]（※モバイルカードでの通信、VPN通信の両方に適用）のうちいずれかを指定します。

■ **方向**

[受信]、[送信]のいずれかを指定します。

■ **動作**

[許可]、[遮断]のいずれかを指定します。

■ **プロトコル**

[全て]、[UDP]、[TCP]、[ICMP]、[ユーザ指定]のいずれかを指定します。
[ユーザ指定]の場合は、プロトコル番号も指定します。

■ **宛先 IP アドレス**

フィルタリングを行う宛先IPアドレスを設定します。

■ **宛先ポート**

フィルタリングを行うポート番号を、1～65535の番号で範囲指定します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字（全角8文字）までの任意の文字列を入力できます。

5. 設定 ボタンをクリックすると、「フィルタリング」リストのページに戻り、設定した内容が反映されます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

メモ フィルタリング設定を工場出荷時の状態に戻す場合は、[初期化]ボタンを押すか、下記の表をご参照いただき、フィルタリングの再設定を行ってください。

表 8-1　工場出荷時のフィルタリングの設定

No.	I/F	方向	動作	プロトコル	宛先 IP アドレス	宛先ポート	メモ
1	全て	送信	許可	TCP		80-80	HTTP
2	全て	送信	許可	UDP		53-53	DNS
3	全て	送信	許可	TCP		25-25	SMTP
4	全て	送信	許可	TCP		110-110	POP3
5	全て	送信	許可	TCP		1720-1720	NetMeeting
6	全て	送信	許可	TCP		1503-1503	NetMeeting
7	全て	送信	許可	TCP		443-443	SSL
8	全て	送信	許可	ICMP		-	ICMP
9	全て	送信	許可	TCP		21-21	FTP
10	全て	送信	許可	UDP		123-123	NTP
11	全て	送信	許可	TCP		23-23	TELNET
12	全て	受信	許可	TCP		23-23	TELNET
13	全て	受信	許可	TCP		80-80	HTTP
14	全て	受信	許可	TCP		21-21	FTP
15	全て	受信	許可	ICMP		ー	ICMP

メモ 工場出荷時では、表 8-1 以外はすべて遮断されます。
それ以外のプロトコルを通過させたい場合は、新たにフィルタリングの設定を行う必要があります。

8.4 バーチャルサーバ

メモ　バーチャルサーバ機能について

バーチャルサーバ機能は、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能です。

通常、LAN に設置されている機器は、ローカル IP アドレスを持っており、グローバル IP アドレスでアクセスを行うことはできません。

バーチャルサーバ機能を利用し、プロトコル・TCP/UDP ポート番号を指定することによって、LAN 内のどの接続機器へ向けての通信であるか特定できるようになるため、グローバル IP アドレスからのアクセスが行えるようになります。

DMZ と同時に使用することは出来ません。

1. 設定ツールのメニューから、[ネットワーク]－[バーチャルサーバ]をクリックします。
「バーチャルサーバ」リストのページが表示されます。

図 8-6　バーチャルサーバ設定リスト画面

2. バーチャルサーバ設定の追加を行いたい場合は、追加 ボタンをクリックします。設定済みの項目を変更する場合は、[変更]をクリックします。
[削除]をクリックすると、表示されている設定が削除されます。
追加 ボタンまたは、[変更]をクリックすると、「バーチャルサーバの詳細設定」ページが表示されます。
追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ　バーチャルサーバの設定は最大 16 件まで行えます。

図 8-7　バーチャルサーバ設定画面

3. 以下の設定を行います。

■ **インターフェイス**

バーチャルサーバの設定を行うインターフェイスを指定します。
指定できるのは、[モバイルカード]のみとなります。

■ **プロトコル**

[TCP]、[UDP]のいずれかを指定します。

■ **ポート番号**

1～65535 までの番号で指定します。
“＊” などのワイルドカードでの指定は行えません。

■ **サーバの IP アドレス**

バーチャルサーバとして外部に公開する機器のIPアドレスを指定します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字（全角8文字）までの任意の文字列を入力できます。

4. 設定 ボタンをクリックすると、「バーチャルサーバ」リストのページに戻り、設定した内容が反映されます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

8.5 DMZ

メモ DMZ 機能について

DMZ 機能は、バーチャルサーバ機能と同様、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能ですが、ポート番号が不明な場合でも設定できます。

ポート番号が特定できない通信を行いたい場合などに最適な設定です。ただし、以下の点にご注意願います。

- Rooster-VMⅡでは、DMZ として設定できる機器は一台のみとなります。
- DMZとして設定された機器には、フィルタリングの設定が（詳細は、☞ 8.3フィルタリングをご覧ください。）全く適用されなくなり、セキュリティが弱くなります。
  必要な場合のみ設定を行うようにしてください。

バーチャルサーバと同時に使用することは出来ません。

1. 設定ツールのメニューから、[ネットワーク]－[DMZ]をクリックします。
   「DMZ」設定のページが表示されます。

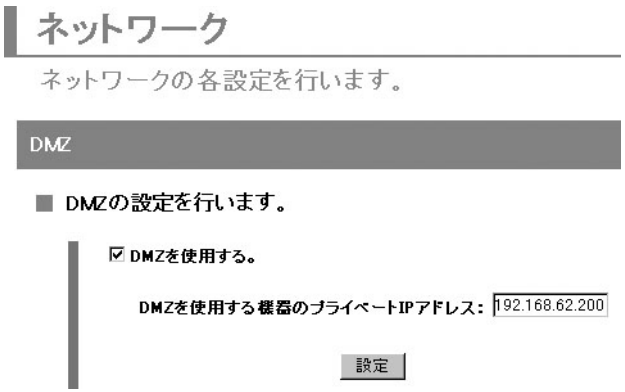


図 8-8　DMZ 設定画面

2. DMZ を使用する場合、「DMZ を使用する。」のチェックをオンにします。
3. 「DMZ を使用する機器のプライベート IP アドレス」に、DMZ として設定する機器のプライベート IP アドレスを入力します。
4. 設定 ボタンをクリックして、設定内容を反映させます。

9. VPN設定

9.1 VPN設定

メモ VPN について

VPN（Virtual Private Network）は、データのカプセル化や暗号化などのセキュリティ技術を使って、インターネットなどの公共的なネットワークで、あたかも専用線接続のような、秘匿性の高いネットワークを実現させるためのしくみです。

Rooster-VMⅡでは、IPsec（IP Security）によるインターネット VPN の構築を行うことができます。

図 9-1　VPN による接続概要図

1. 設定ツールのメニューから、[ネットワーク]－[VPN]をクリックします。
   「VPN」リストのページが表示されます。

図 9-2　VPN 設定リスト画面

2. VPN 設定の追加を行いたい場合は、追加 ボタンをクリックします。設定済みの項目を変更する場合は、[変更]をクリックします。
   「VPNの詳細設定」ページが表示されます。

メモ VPN の設定は最大 16 件まで行えます。

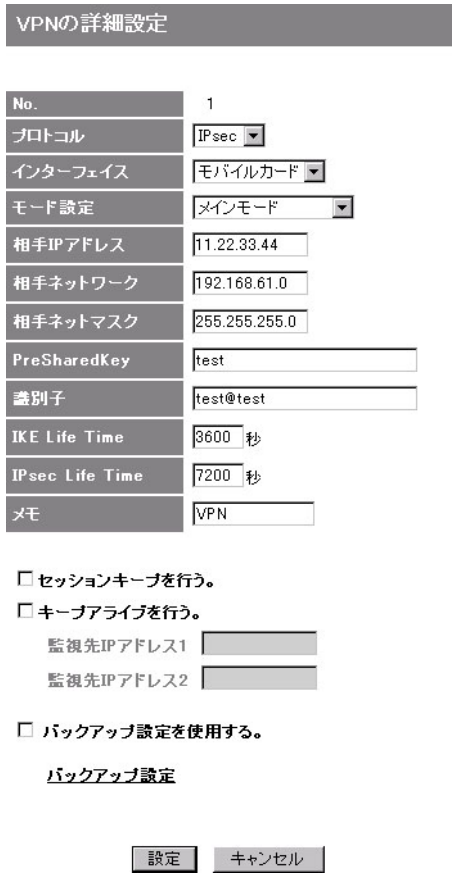


図 9-3　VPN 設定画面

3. 以下の設定を行います。

■ **プロトコル**

対応プロトコルはIPsecのみで固定となります。

■ **インターフェイス**

この設定を適用するインターフェイスを選択します。
[モバイルカード]のみ設定できます。

■ **モード設定**

メインモード、あるいはアグレッシブモードを選択します。

注意 2 点間の VPN 接続で、少なくともいずれか一方は、固定 IP サービスなど、グローバル IP アドレスが不変の環境でなければ接続できません。

- 2 点間共に固定 IP アドレスが不変⇒メインモードで設定します。
- 一方が固定 IP アドレス、他方が接続するたびに IP アドレスが変動する⇒アグレッシブモードで設定します。

■ **相手 IP アドレス**

IPsec通信を行う相手先のグローバルIPアドレスを指定します。

■ **相手ネットワーク**

IPsec通信を行う相手先のローカルネットワークアドレスを指定します。

■ **相手ネットマスク**

IPsec通信を行う相手先のローカル(サブ)ネットマスクアドレスを指定します。

■ **PreSharedKey**

IPsec通信を行うために使用する認証用キーフレーズを設定します。
2点間で同じ値を設定します。

■ **識別子**

アグレッシブモードで接続する際に、IPsec通信で互いに相手を識別するために設定します。2点間で同じ値を設定します。

■ **IKE Life Time**

IKEの寿命を秒単位で指定します。

■ **IPsec Life Time**

IPsecの寿命を秒単位で指定します。

■ **セッションキープを行う**

チェックをオンにした場合、VPN接続が切断されると、自動的に再接続を行うようになります。

■ **キープアライブを行う**

VPN接続を常時監視し、接続状態を続ける機能です。
チェックをオンにした場合、VPN接続時に接続確認のために、設定された監視先IPアドレスにpingパケットを発信するようになります。

注意 セッションキープ、キープアライブは、従量制課金でご契約の場合は、設定しないようにしてください。
意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

■ **バックアップ設定を使用する**

上記の設定で接続できなかった場合、代替の設定で接続を行うようにすることができます。代替の設定を使用する場合、チェックをオンにします。

> **注意** 引き続いて「バックアップ設定」も行う場合は、ここで一度、 設定 ボタンをクリックして、設定内容を反映させます。
> **先にクリックすると、設定した内容が破棄されてしまいます。**

4. 設定 ボタンをクリックすると、「VPN」リストのページに戻り、設定した内容が反映されます。
   キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

> **注意**
> - 設定が空白の場合、自動的に適切な設定が行われるようになっていますが、念のために、メインモード、アグレッシブモードに関わらず、メモ以外のすべての項目について設定を行ってください。
> - VPN の接続が完了するまでに1～3 分程度かかります。
>   通信を行う前に、ping コマンド等で接続状態を確認することをお勧めします。

- 他社製 VPN 機器と接続を行う場合、以下の表を参考に設定を行ってください。

表 9-1　Rooster-VMⅡ　既定の VPN 接続設定

項目	既定の設定内容
基本設定	
データ圧縮 (IPCOMP プロトコル)	圧縮は使用しない
鍵交換方式	IKE（Internet Key Exchange)を使って、SA の合意を通信時に自動的に行う (手動設定は行わない)
IKE フェーズ 1 (ISAKMP SA の作成) の設定	
接続試行回数	無限回(制限なし)
ハッシュアルゴリズム	SHA-1、MD5
認証(本人性確認)方式	Pre-Shared Key (共通鍵) 認証方式
Pre-Shared Key (共通鍵) の設定	自分側と相手側両方に、同じキーフレーズを設定。
暗号化アルゴリズム	3DES
Diffie-Hellman-Group	DH Group 2
識別子 (ホスト ID)	ホスト ID を設定
IKE Life Time	経過時間による設定のみ
IKE フェーズ 2 (IPsec SA の作成) の設定	
セキュリティプロトコル	ESP のみ
IPsec Life Time	経過時間による設定のみ
カプセル化モード	トンネリングモード
暗号化アルゴリズム	3DES
ハッシュアルゴリズム	SHA-1、MD5
PFS (Diffie-Hellman の再計算)	行わない

9.2 VPN通信の接続/切断方法

1. 設定ツールのメニューから、[ステータス 接続/切断]－[VPN] をクリックします。
   VPNステータスのページが表示されます。

図 9-4　VPN ステータス表示画面

■ **No.**

VPN設定の通し番号が表示されます。

■ **相手 IP アドレス**

IPsec通信を行う相手先のグローバルIPアドレスが表示されます。

■ **相手ネットワーク**

IPsec通信を行う相手先のローカルネットワークアドレスを指定します。

■ **メモ**

メモに設定された文字列が表示されます。

■ **ステータス**

設定したダイヤルアップ接続の現在の状態が表示されます。
[詳細表示]をクリックすると、現在の状態をより詳しく参照できます。

● **ステータス一覧**

ステータス表示	状態	VPN ランプの状態
無効	VPN 設定が無効になっています。	消灯
待機中	VPN 接続設定は行われていますが、VPN 接続を試みていない状態です。	消灯
接続試行中	VPN 接続を行おうとしています。 この状態が長く続く場合、設定が間違っているか、相手側がオフラインになっている等の問題で接続できない可能性があります。	消灯
接続完了	VPN 接続が正常に行えた状態です。	点灯

■ **操作**

それぞれ以下の操作を行います。

- [接続]⇒接続動作を行います。
- [切断]⇒切断動作を行います。
- [無効]⇒設定を無効にします。
  次回、[有効]をクリックするまで設定内容を使えないようにします。
- [有効]⇒設定を有効にします。
  次回、[無効]になっている設定を再度使えるようにします。

9.2.1 2点間のWAN側IPアドレスが固定の場合

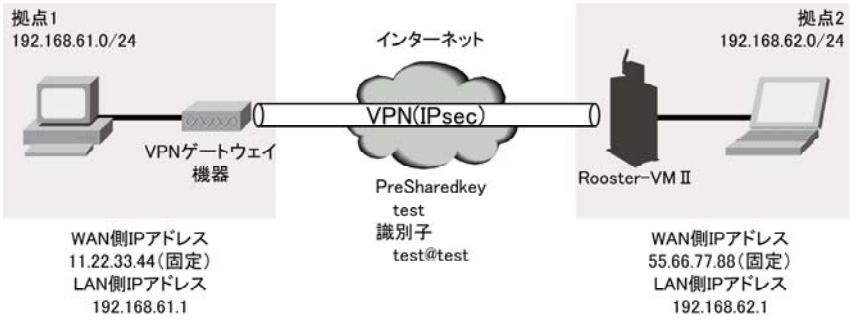


図 9-5 2 点間の WAN 側 IP アドレスが固定の場合

● Rooster-VM Ⅱの設定例

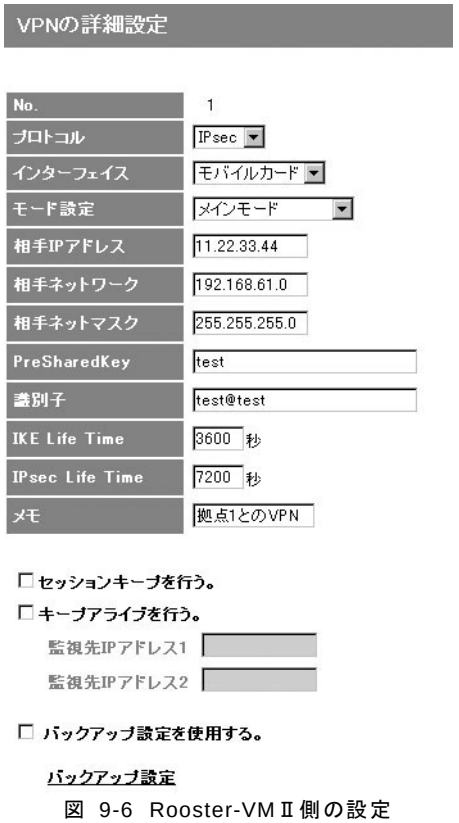


図 9-6 Rooster-VM Ⅱ側の設定

9.2.2　WAN側IPアドレスの一方が固定、Rooster-VMⅡが動的の場合

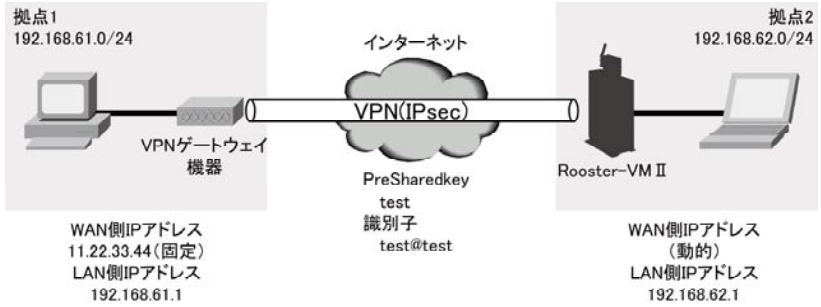


図 9-7 WAN 側 IP アドレスの一方が固定、Rooster-VMⅡが動的の場合

- Rooster-VMⅡの設定例

図 9-8 Rooster-VMⅡ側の設定

10. ログの参照方法

10.1 パケット通信ログ

> **注意** 工場出荷時状態では、Rooster-VMⅡへの負荷を軽減させるため、パケット通信ログは記録しない設定になっています。
>
> パケット通信ログを記録させる場合は、[ログ管理]の設定で「ログ管理を行う」のチェックをオンに設定してください。
>
> （設定方法は、☞ 7.9ログ管理をご覧ください。）

10.1.1　パケット通過ログ

設定ツールのメニューから、[ログ]－[パケット通信ログ] －[通過ログ]をクリックします。
パケット通過ログ一覧のページが表示されます。

図 10-1　パケット通過ログ一覧画面

■ **No.**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **通信タイプ**

IPパケットの種別（TCP、UDP、ICMPなど）が表示されます。

■ **発信元 IP**

通信の起点になる機器のIPアドレスが表示されます。

■ **発信元ポート**

通信の起点になる機器の使用ポート番号が表示されます。

■ **送信先 IP**

通信の宛先になる機器のIPアドレスが表示されます。

■ **送信先ポート**

通信の宛先になる機器の使用ポート番号が表示されます。

■ **終了した理由**

通信が終了した理由が表示されます。

正常終了
⇒正常に通信が行われた時に表示されます。
タイムアウト
⇒通信セッション確立後、通信が途中で終了、あるいは終了フラグを確認できなかった時に表示されます。

10.1.2 パケット遮断ログ

設定ツールのメニューから、[ログ]－[パケット通信ログ] －[通過ログ]をクリックします。
パケット遮断ログ一覧のページが表示されます。

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート
1	2005/01/19 18:07:04	UDP	192.168.62.50	3040	11.22.33.44	123
2	2005/01/19 18:11:38	TCP	192.168.62.50	3221	11.22.33.44	23
3	2005/01/19 18:11:48	TCP	192.168.62.50	3221	11.22.33.44	23
4	2005/01/19 18:12:17	TCP	192.168.62.50	3234	11.22.33.44	445
5	2005/01/19 18:12:23	TCP	192.168.62.50	3234	11.22.33.44	445

図 10-2 パケット遮断ログ一覧画面

■ **No.**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **通信タイプ**

IPパケットの種別（TCP、UDP、ICMPなど）が表示されます。

■ **発信元 IP**

通信の起点になる機器のIPアドレスが表示されます。

■ **発信元ポート**

通信の起点になる機器の使用ポート番号が表示されます。

■ **送信先 IP**

通信の宛先になる機器のIPアドレスが表示されます。

■ **送信先ポート**

通信の宛先になる機器の使用ポート番号が表示されます。

10.2 回線ログ

10.2.1 モバイルカードログ

設定ツールのメニューから、[ログ]－[回線ログ] －[モバイルカードログ]をクリックします。
モバイルカードログ一覧のページが表示されます。

No.	記録時間	ログ
1	2005/01/19 17:37:26	モバイルカード制御サービスを開始します
2	2005/01/19 17:37:37	モバイルカードをDDIPカードとして認識しました
3	2005/01/19 17:37:56	--- モバイルカードを初期化します ----------
4	2005/01/19 17:38:00	ダイヤルを行ないます
5	2005/01/19 17:38:00	電話番号: 0570-111-111##64
6	2005/01/19 17:38:06	回線接続が確立しました
7	2005/01/19 17:38:30	PPP接続が確立しました

図 10-3 モバイルカードログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

モバイルカードの動作状態が表示されます。
ダイヤルアップ接続、およびRAS着信接続が正常に行えない場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。

受信：NO CARRIER
回線接続の確立に失敗しました（リザルトエラー）

⇒以下のいずれかの場合が考えられます。

1. ダイヤルアップ接続先の電話番号が間違っている。

   ⇒正しい電話番号を設定してください。

2. 電波状態が悪い。

   ⇒Rooster-VMⅡを通信状態のよい場所に移動するか

   （できるだけ窓側あるいは高い場所）
   あるいは、しばらく時間を置いてやり直してみてください。

受信：DELAYED
回線接続の確立に失敗しました（リザルトエラー）

⇒3分間以内に3回以上、同一電話番号に電話を掛けようとすると、
モバイルカードに発信規制が掛かってしまいます。
一旦接続動作を解除して、しばらくお待ちいただいてからお掛け直しください。

PPP 接続でユーザ認証に失敗しました

⇒ダイヤルアップ接続のID、パスワードのいずれかに誤りがあります。
再度、ダイヤルアップ接続の設定の確認を行ってください。

電話番号認証に登録がありません
着信条件が合わない為、無視します

⇒RAS着信相手先リスト画面に登録されていない電話番号のため、
相手からの着信要求を無視しています。
RAS着信相手先リストに該当する番号を登録するか、着番認証のチェックをオフに設定してください。

10.2.2 VPNログ

設定ツールのメニューから、[ログ]－[回線ログ] －[VPNログ]をクリックします。
VPNログ一覧のページが表示されます。

図 10-4 VPN ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

VPNの動作状態が表示されます。
VPN接続が成功すると、「IPsecのNo.＊（＊はVPN設定リストのNo.）が接続完了しました」と表示されます。
接続できない場合、VPNの設定に誤りがないかどうかご確認ください。
VPNの設定につきましては、☞ 9.1 VPN設定をご覧ください。

10.3 サービスログ

10.3.1　アドレス解決ログ

設定ツールのメニューから、[ログ]－[サービスログ] －[アドレス解決ログ]をクリックします。
アドレス解決ログ一覧のページが表示されます。

図 10-5　アドレス解決ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

アドレス解決機能の動作状態が表示されます。
「アドレス解決プロセスは異常終了しました」となる場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。

● **アドレス解決をメール送信で行っている場合**

SMTP サーバ エラー：535 Error: authentication failed

ユーザ認証SMTPのメールサーバで、[本体設定]-[メールアカウント設定]の、「アカウント」、「パスワード」のいずれかに誤りがある場合に表示されます。

SMTP サーバ エラー：501 Syntax: MAIL FROM:

ユーザ認証SMTPのメールサーバで、[各種サービス]-[アドレス解決]の、「送信元メールアドレス」の設定がされていないか、書式に誤りがある場合に表示されます。

SMTP サーバ エラー：572 Relay not authorized

POP before SMTPのメールサーバで、[本体設定]-[メールアカウント設定]の「サービスの種類」に「ユーザ認証SMTP」の設定を行った場合に表示されます。

● **アドレス解決を DynDns で行っている場合**

DynDns サーバ エラー ：HTTP/1.1 401 Authorization Required

DynDNS設定の、アカウント、パスワードのいずれかに誤りがある場合に表示されます。
ホスト名に誤りがある場合は表示されず、異常終了のログのみ表示されます。

10.3.2　DHCPログ

設定ツールのメニューから、[ログ]－[サービスログ]－[DHCPログ]をクリックします。DHCPログ一覧のページが表示されます。

図 10-6　DHCP ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

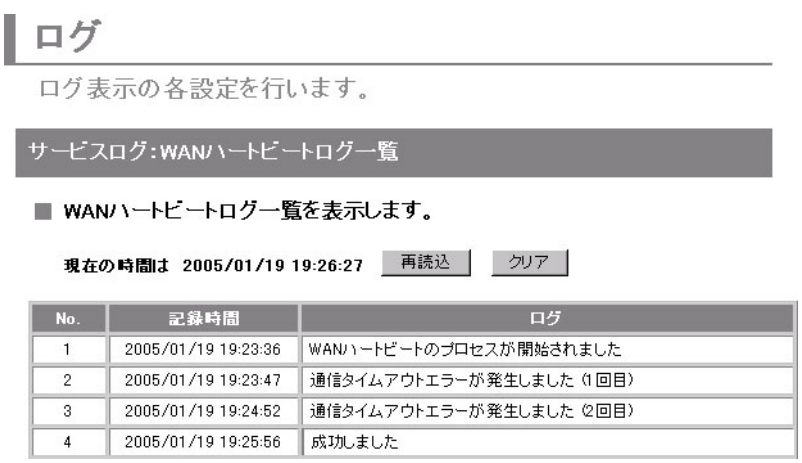
時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

DHCP機能の動作状態が表示されます。

10.3.3 WANハートビートログ

設定ツールのメニューから、[ログ]－[サービスログ]－[WAN]ハートビートログをクリックします。WANハートビートログ一覧のページが表示されます。


ログ

ログ表示の各設定を行います。

サービスログ:WANハートビートログ一覧

■ WANハートビートログ一覧を表示します。

現在の時間は 2005/01/19 19:26:27 再読込 クリア

No.	記録時間	ログ
1	2005/01/19 19:23:36	WANハートビートのプロセスが開始されました
2	2005/01/19 19:23:47	通信タイムアウトエラーが発生しました (1回目)
3	2005/01/19 19:24:52	通信タイムアウトエラーが発生しました (2回目)
4	2005/01/19 19:25:56	成功しました

図 10-7 WAN ハートビートログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

WANハートビート機能の動作状態が表示されます。

10.3.4 PPPログ

注意 工場出荷時状態では、Rooster-VMⅡへの負荷を軽減させるため、PPPログは記録しない設定になっています。

PPPログを記録させる場合は、[ログ管理]の設定で「PPPログを有効にする」のチェックをオンに設定してください。

（設定方法は、☞ 7.9ログ管理をご覧ください。）

設定ツールのメニューから、[ログ]－[サービスログ] －[PPPログ]をクリックします。
PPPログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

サービスログ:PPPログ一覧

■ PPPログ一覧を表示します。

現在の時間は 2007/10/30 14:40:46 再読込 クリア

No.	記録時間	ログ
1	2007/10/30 14:40:11	pppd options in effect:
2	2007/10/30 14:40:11	debug # (from /etc/ppp/peers/ppp_client)
3	2007/10/30 14:40:11	kdebug 0 # (from command line)
4	2007/10/30 14:40:11	idle 600 # (from command line)
5	2007/10/30 14:40:11	persist # (from command line)
6	2007/10/30 14:40:11	demand # (from command line)
7	2007/10/30 14:40:11	logfile sclog # (from /etc/ppp/peers/ppp_client)
8	2007/10/30 14:40:11	unit 1 # (from command line)
9	2007/10/30 14:40:11	dump # (from /etc/ppp/peers/ppp_client)
10	2007/10/30 14:40:11	user test # (from command line)
11	2007/10/30 14:40:11	/dev/ttyS0 # (from command line)
12	2007/10/30 14:40:11	115200 # (from command line)
13	2007/10/30 14:40:11	lock # (from command line)
14	2007/10/30 14:40:11	connect /rooster/ondemand.sh # (from command line)
15	2007/10/30 14:40:11	crtscts # (from command line)

図 10-8 PPP ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

PPPの動作状態が表示されます。

10.4 その他ログ

10.4.1　システムログ

設定ツールのメニューから、[ログ]－[その他ログ] －[システムログ]をクリックします。
システムログ一覧のページが表示されます。

図 10-9　システムログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

Rooster-VMⅡのシステムに関するログが表示されます。

製品仕様

製品名		Rooster-VMⅡ
型名		SC-RS920VM2
JAN コード		4582131720188
ルーティング方式		スタティックルーティング ダイナミックルーティング
インターフェイス		MDI/MDI-X 自動判別
	LAN ポート	100BASE-TX/10BASE-T ×4 ポート
	メンテナンス ポート	100BASE-TX/10BASE-T ×1 ポート
	PCMCIA ポート	TypeⅡ準拠（3.3/5V 両対応）×1 ポート
ハードウェア 構成	CPU	SH7710（200MHz）
	メインメモリ	32MB
	フラッシュメモリ	8MB
リセットスイッチ		1 個
電源仕様		AC アダプタ
	定格入力	AC100V（50/60Hz）
	定格出力	DC1.0A（DC12V）
	最大消費電力	7.5W
環境条件	温度	5～40℃
	湿度	25～85%（結露なきこと）
	耐ノイズ性 ※1 AC ラインノイズ DC ラインノイズ	 ±2000V パルス幅 100ns/1000ns ±2000V パルス幅 100ns/1000ns ノイズシュミレータによる ※フェライトコア非接続時
	耐静電気性性※1 直接放電 気中放電	 ±10KV LAN 端子金属部 ±10KV LAN 端子金属部
重量		約 470g（付属品含まず）
外形寸法		30（W）×140（H）×100（D）mm（縦置き時） （付属物/ケーブル/突起物は含まず）

サポート プロトコル	Ethernet	CSMA/CD
	ルーティング	IP のみ
	認証	PAP、CHAP、MS-CHAPv2
	暗号化プロトコル	MPPE128bit
	WAN プロトコル	PPP
	管理プロトコル	SNMPv1
	ルーティング プロトコル	RIP v1、v2
WAN 接続方式		Numbered、Unnumbered、ビジネス mopera
DHCP		● サーバ機能（LAN 側最大 253 クライアント） ● リレー機能
アドレス変換		NAT/IP マスカレード
VPN パススルー		IPsec/PPTP パススルー
サーバ公開		● バーチャルサーバ（最大 16 件設定可） ● DMZ ホスト（1 件設定可）
スタティックルーティングテーブル		最大 32 件登録可能
アップデート		WWW ブラウザによるアップデート
WakeOn 着信	メッセージ 認証登録	メッセージ登録（128 文字）/1 件
	着信番号登録	CLID/16 件
アドレス解決	アドレス登録	1 件
	メッセージ登録	1 件
	プロトコル	SMTP、POP
	ダイナミック DNS	どこでもカメラ、DynDNS、Suncomm.DDNS
	更新時間設定	可能（5 分～）
WAN ハートビート	相手先	WAN ゲートウェイ、任意のアドレス設定
	更新時間設定	可能（1 分～）
無通信監視タイマー		設定可能

電源制御		● ハードウェアおよびソフトウェア ● モバイルカード ※本体電源 OFF から 10 秒±5 秒で電源 ON
ダイヤルアップ自動発信条件		● LAN 側からのパケット送出 ● ダイヤルアップ/セッションキープ ● ダイヤルアップ/キープアライブ ● IPsec/セッションキープ ● IPsec/キープアライブ ● WAN ハートビート ● NTP
ダイヤルアップ手動発信/切断		可能
ダイヤルアップ先設定		1 件
ダイヤルアップセッションキープ		可能
リモートアクセス	プロトコル	PIAFS2.2/2.1/2.0/1.0/FOMA64K （モバイルカードに依存）
	着信番号登録	CLID/50 件
	認証方式	CLID ×50 件、PAP、CHAP
VPN 機能	暗号化	IPsec（VPN 機能）＋3DES
	アルゴリズム	ハードウェア処理 IKE（メインモード、アグレッシブモード）
	接続可能数	最大 16 件
	セッションキープ設定	可能
	キープアライブ設定	可能
	バックアップ設定	別 VPN 装置への接続設定可能（1 セッションにつき 1 件）
	LifeTime 設定	可能
QoS 機能		優先制御、帯域制御
		IP アドレス、ポート番号
		最大 8 件登録可能

ロギング		● WWW ブラウザによる各種ログ表示 ● Syslog での出力
ログの内容		● パケット通信ログ ● パケット遮断ログ ● モバイルカードログ ● アドレス解決ログ ● WAN ハートビートログ ● PPP ログ ● VPN ログ ● システムログ
設定情報管理		● WWW ブラウザによるファイル保存、読み込み ● telnet 上でのコマンドによる読み込み、書き込み
パケットフィルタリング		最大 32 件登録可能 以下の各パラメータによるフィルタリング ● インターフェイス ● 方向 ● 動作 ● プロトコル ● 宛先 IP アドレス ● 宛先ポート ● 許可または遮断
ファームウェア設定		WWW ブラウザ、TELNET による設定
インターネット経由のリモートセットアップ		可能
時刻管理	設定方法	NTP サーバ設定/手動設定
	更新時間設定	可能
保証		1 年間

付属品	● スタートアップマニュアル---1 部 ● CD-ROM（取扱説明書類収録）---1 枚 ● 保証書---1 枚 ● AC アダプタ---1 個 ● UTP ケーブル（カテゴリ 5 ストレート）---1 本 ● 電源プラグ抜け防止クランプ---1 個 ● 本体固定用ステー---2 枚 ● モバイルカード保護板---1 枚 ● FG 用ネジ---1 個 ● 固定用ネジ--- 6 個 ・固定用ステー用---4 個 ・PC カード保護板用---2 個 ● ゴム足---4 個

※1　ノイズを印加し続けた際の動作を保証するものではございません。

サポートのご案内

● **最新情報の入手**

Rooster-VMⅡに関する最新情報は、弊社ホームページから入手することができます。
また、バージョンアップ情報につきましても公開しております。

■ **製品紹介ページ**

http://www.sun-denshi.co.jp/sc/rooster_vm2/

● **ご質問・お問い合わせ**

Rooster-VMⅡに関するご質問やお問い合わせは、下記へご連絡願います。

サンコミュニケーションズ　サポートセンター

- 電話　0587-55-0161
- FAX　0587-55-0815
- メール　support-suncomm@sun-denshi.co.jp
- 受付時間　月曜～金曜　10:00～16:00（12:00～13:00 を除く）
  祝祭日、弊社休日を除く

Rooster-VMII

SC-RS920VM2
取扱説明書　Ver.1.3

2009 年 6 月発行

サン電子株式会社

〒483-8555　愛知県江南市古知野町朝日 250
※無断複写・転載を禁止します。

(090619)